

# Expanding the UK Secure by Design proposal for a usable consumer-focused IoT security label

Mathew Estienne



Masters by Research, Cyber Security



**Swansea University**  
**Prifysgol Abertawe**

Department of Computer Science

Adran Gyfrifidureg

August 28, 2023

Copyright: The Author, Mathew Estienne, 2023

Distributed under the terms of a Creative Commons Attribution 4.0 License (CC BY 4.0).

# Declaration

## Statement 1

This work has not been previously accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed Mathew Estienne ( [REDACTED] )

Date August 28, 2023

## Statement 2

This thesis is the result of my own investigations, except where otherwise stated. Other sources are acknowledged by citations giving explicit references. A bibliography is appended.

Signed Mathew Estienne ( [REDACTED] )

Date August 28, 2023

## Statement 3

The University's ethical procedures have been followed and, where appropriate, ethical approval has been granted.

Signed Mathew Estienne ( [REDACTED] )

Date August 28, 2023

“A commercial, and in some respects a social, doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery. Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done.

If a lock (let it have been made in whatever country, or by whatever maker) is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to be the first to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance. It cannot be too earnestly urged, that an acquaintance with real facts will, in the end be better for all parties.”

*A.C. Hobbs*

*Rudimentary treatise on the construction of locks*

1853

## **Abstract**

No person whom has any knowledge of security in the Internet of Things (IoT) would claim the current landscape is desirable, as exceedingly poor security of devices is routinely exhibited in an ecosystem experiencing exponential growth of devices. If these devices follow past trends in Cyber Security, it is not unreasonable to assume that without intervention another decade of exponentially growing costs attributed to Cyber Crime may lay ahead. After the failure of the voluntary approach to IoT Security, works are now being taken to legislate a minimum security standard.

Building from existing proposals, this paper outlines real improvements that could be made to current ongoing works, with the intention of providing incentive for manufacturers to improve device security in the IoT sector and reduce the timeline for routine deployment of secured devices.

Incorporating strategies developed in other industries, as well as security requirements from across international borders, a point-of-sale user focused label is proposed, which can be easily interpreted by non-technical users. Intending to provoke curiosity and fully reassure the end-user, a two-layer system is chosen which allows the conveyance of more detailed information than could fit on a physical label.

# Contents

- I Introduction 5**
- 1 Rationale for Cybersecurity research and corrective actions ..... 5
  - 1.1 The Internet of Things; Why focus efforts here? ..... 5
- 2 Contributions ..... 9
  
- II Understanding UK IoT “Secure by Design” in a Cybersecurity context 10**
- 3 Existing Proposals ..... 10
  - 3.1 UK Proposal Overview ..... 10
  - 3.2 EU Proposal Overview ..... 12
- 4 Relevant Works to understanding the Cybersecurity context ..... 14
  - 4.1 A note on QR Codes ..... 16
- 5 Existing Proposal Analysis and Deconstruction ..... 17
  - 5.1 Analysis of UK IoT “Secure by Design” Requirements ..... 17
  - 5.2 Mapping UK IoT “Secure by Design” into ENISA Baseline Security Requirements for IoT ..... 25
- 6 Suitability of Existing Proposal ..... 38
  - 6.1 Existing device classification ..... 38
  - 6.2 Interpretation ..... 42
  
- III Improving UK IoT “Secure by Design” proposal through international standards 44**
- 7 Improving the Requirements ..... 44
  - 7.1 European Requirement Mapping and Unmappable Requirements ..... 44
  - 7.2 Expanding Requirements ..... 45
  - 7.3 Finished Categories ..... 58
- 8 Existing device reclassification ..... 62
  
- IV Developing a usable IoT Cyber Security label for point-of-sale solutions 64**
- 9 Existing Label Proposal ..... 65
  - 9.1 Why is a label the preferred catalyst for security improvement in IoT devices? ..... 65
  - 9.2 Process to acquire Harris Interactive proposed label ..... 66
  - 9.3 Discussion Points ..... 67
    - 9.3.1 Potential alternate processes involving Harris Interactive proposed label ..... 67
    - 9.3.2 Label ..... 69
    - 9.3.3 Why the current label is insufficient; Additional information to take into account when trying to determine the structure of a new label ..... 70
  - 9.4 Key characteristics identified and label objectives ..... 71
- 10 Own Proposed Label ..... 72
  - 10.1 Main Proposal ..... 72
  - 10.2 Alternate Proposal ..... 74
  - 10.3 Label 1.0 ..... 75
- 11 Prototype testing ..... 78
  - 11.1 User Studies ..... 78
  - 11.2 Focus Group Interviews ..... 82
    - 11.2.1 Cyber Professionals ..... 82
    - 11.2.2 Cyber Academics ..... 83
- 12 Revised Label Specification ..... 84

<b>V</b>	<b>Conclusions and Future Improvements</b>	<b>92</b>
13	Summary .....	93
14	Future Work .....	93
14.1	Mappings between Additional Security Standards .....	93
14.2	Further User-Based Research .....	94
14.3	Subcategorisation based on external input .....	96
<b>VI</b>	<b>Appendices</b>	<b>108</b>
15	Survey Files .....	108
16	Focus Group Files .....	108
17	Raw Image Files .....	109
17.1	Survey Figures .....	109
17.2	Label Icons .....	109
17.3	Fullsize Document Figures .....	110

## Part I

# Introduction

## 1 Rationale for Cybersecurity research and corrective actions

Every invention of a secure system is also an invitation to those who would challenge it, whether the creator realises it or not. The world of computing is a new one, and as such not all lessons learnt in other disciplines have yet made their way across. Shop owners do not leave their stock unguarded at night, governments keep sensitive records in secure filing systems and Operational Security is a well established principle in the armed forces [1]. Yet, as the majority of the world's population were raised without computers [2, 3], this natural "common sense" has yet to permeate globally. Adding to this societal unpreparedness for such an interconnected world, corporations have been reactive [4] in their response to cyber threats, rather than proactive. For example, the Windows NT Kernel (which Microsoft Windows builds upon even now [5]) was developed before malware had ever been deployed for malicious purpose [6, 7, 8]. As such, it was not designed with such threats in mind and consequently throughout the 2000s it was "normal" to have your computer compromised [9], with the expectation that a user simply remove the infection with a third party anti-virus program. Patch Tuesday for Windows is infamous as a monthly patching of newly discovered security vulnerabilities [10]; there is an expectation that the currently deployed software is going to be compromised, and that there will be so many incidents exploiting different vulnerabilities that inconvenience to users for updating has had to be factored in, rolling updates into bulk and deploying on a regular, recurring timeline.

General purpose computers are now beginning to incorporate resilience against cyber attacks into their designs, the first out-of-the-box protections deployed before a user asks for them rather than being reactive [11]. While things are far from ideal, and there are still innumerable avenues for attack, it is far rarer for a computer to be compromised without some form of user error. Security has reached a level where a "normal user" may use their computer for simple tasks without compromising their system in the process, but they would have no resilience against a targeted attack. However, it can be stated that (generously) this has taken 20 years of users being left vulnerable, with a tremendous cost to both corporations and the individual [12]. Now, the Internet of Things has emerged, and is seemingly set to take a similarly long time to develop adequate security precautions and procedures [13]. After ten years, there is still just talk of changes and regulation, but devices are patched reactively (if they are patched at all) rather than secured by design. Meanwhile, as of 2020, the total cost of cybercrime has now crossed 1% of global GDP, surpassing projections from 2018 by 50% [14].

### ***1.1 The Internet of Things; Why focus efforts here?***

The Internet of Things is defined in the Oxford English Dictionary as "a proposed development of the internet in which many everyday objects are embedded with microchips giving them network connectivity, allowing them to send and receive data." [15]. Although first coined as a phrase describing a hypothetical, it has rapidly developed from a niche into mass market adoption. As of 2020, there are now more IoT devices connected to the internet than the cumulative total for all other types of device [16].

Three primary factors were responsible for the rapid growth of the Internet of Things. The increasing awareness that big data has incredible value [17, 18], particularly when it can be paired with machine learning. This has created an incentive for corporations to gather as much as possible, from anywhere possible. The growth of the miniature electronics market due to the advent of the smartphone, featuring high efficiency parts produced en-masse, with no expectation of an attached bulky interface [19]. This reduced the manufacturing costs [20] for deployment of data collection devices [18]. Finally, the expansion of internet coverage that can support a relatively consistent data stream [21]. This allows the retrieval of that data, with near zero cost, in tremendous quantities [22]. As the primary motive of manufacturing these devices has been to retrieve that valuable data, the development of the Internet of Things has thus-far had more in common with a gold rush than the kinds of organised deployments that the world of computing was previously familiar with. The low cost to produce allows rapid iteration of physical devices [23], while the internet connection allows updating of software without an expensive recall of devices. By the time investigation is concluded on a device and consumers made aware of flaws, the company may have already shipped a successor device, and the issue buried. This leaves those elsewhere to bear the cost, with incredible security breaches and financial loss occurring at record breaking levels year-on-year [24].

When attempting to accurately determine the true scale of Cyber Attacks, it is difficult to even estimate the true number of attacks against IoT devices and how many devices may be compromised. Given the goal of most of these attackers is to remain undetected (such that access may be retained for future use), it is likely that a significant proportion of those compromised are unaware. Additionally, many businesses whom are compromised may choose to withhold this information from the general population, for fear of financial impacts [25, 26]. As such, relying on reports from defenders of their own compromised devices is likely to leave large gaps in the data [27]. Relying on attackers to self-report the numbers of devices they have compromised is also likely to result in inaccurate figures. Hackers may boast and claim large numbers of compromised devices for “marketing” of their services, inflating their numbers [28]. Conversely, those not in the business of marketing their abilities are unlikely to want to report their activities. Reporting is in-fact so unreliable that it is inadvisable to even try and negate opposing factors, as estimates may have error to orders of magnitude [28].

Bearing all these factors in mind, the most well regarded statistics around cybercrime in the cybersecurity world come from Honeypots [28]. These have their own inaccuracies and limitations, however the results from honeypots are more likely to fall within “sane” values (upper estimates not exceeding total number of devices sold, or lower estimates below known compromised devices from alternate sources). However, this author advises that numbers from honeypots should still always be regarded with a degree of scepticism, and such factors taken into account as the following statistics are discussed.

The Oxford English Dictionary defines Exponential Growth as “growth whose rate becomes ever more rapid in proportion to the growing total number or size.” [30]. Bearing the aforementioned important considerations in mind, data obtained of attacks on IoT devices exhibit this behaviour, with rapid growth on the y-axis rapidly diminishing any previously impressive value from prior years. It can be hard for the human mind to comprehend exponential growth [31], a lesson further reinforced during decisions made around the world during the Covid-19 pandemic, which may be a contributing factor to the delay in action from the legislature when tackling a problem with such a growth rate. However, [31] shows that simple visualisation of the data can help quite effectively to reduce the handicap when analysing exponential trends. Figure 2 and Figure 3 are provided to aid with this.

In 2017, with the 2016 Mirai Internet of Things botnet making headlines, this was the first time an attack on IoT devices had made it’s way into the public consciousness. There had been prior cyberattacks and botnets involving IoT devices [34], but the fact that properties inherent to the Internet of Things were making them prime targets for slaving to a botnet was being noticed. Always on devices, with a permanent internet connection, copy-paste designs and largely unmonitored by both users and system administrators.

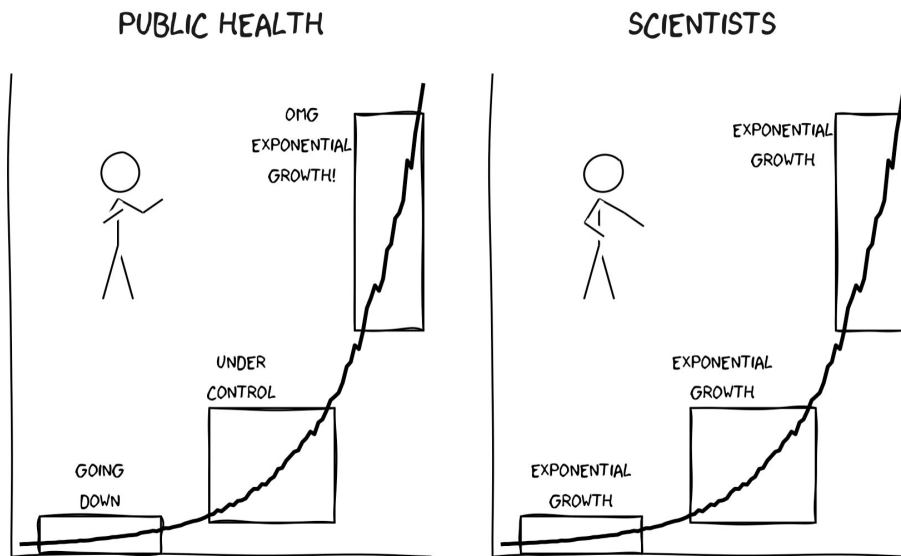


Figure 1: Public Health vs Scientists [29]. An illustration of how a trend of exponential growth may be interpreted differently by those without experience (made specifically in reference to Covid-19 pandemic response)

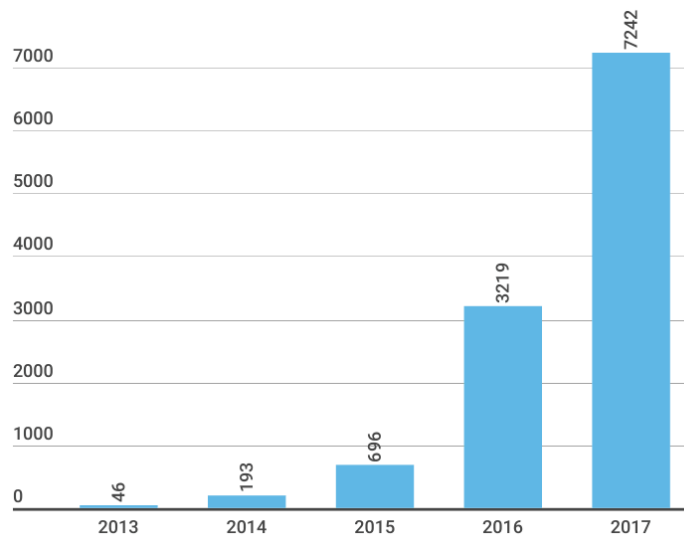


Figure 2: 'Internet of Things' Malware Collection by Kaspersky Lab's IoT honeypots until Q2 2017 [32]



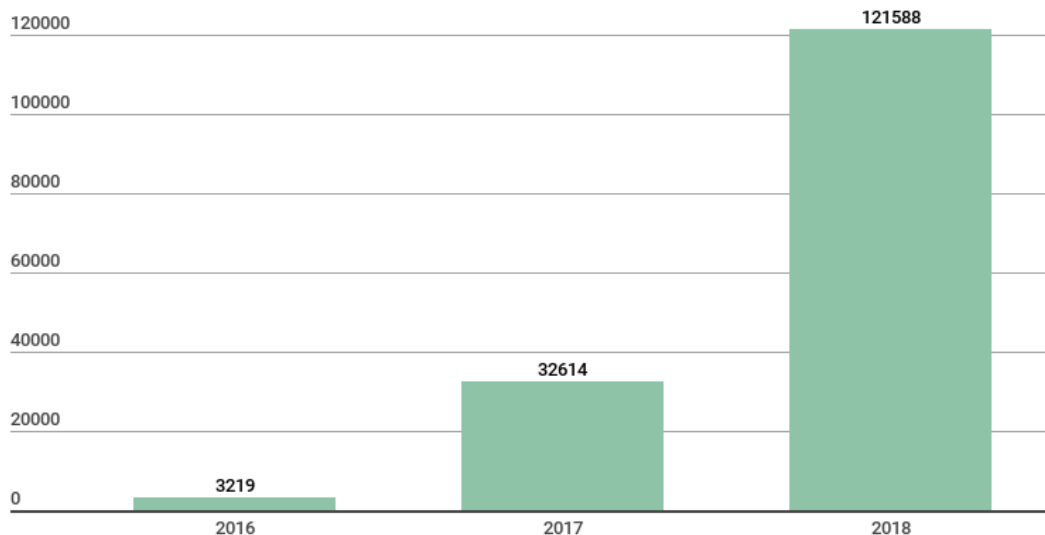


Figure 3: IoT Malware Collection by Kaspersky Lab's IoT honeytraps until Q2 2018 [33]

The insecure nature of these IoT devices making their way out into the general public had already been raised as an issue [35, 36, 37], Cyber Security organisations had already recommended action [38, 39] (which coincidentally seems eerily familiar to the advice still not being heeded in 2021) and had begun preparations for the expansion of work in the sector [40, 41], but this was the first attack of sufficient scale to garner additional attention. As such, predictions for the future were for increases in Cyber Security breaches in this new zone of interest [42]. Estimates varied wildly, but few reputable sources would have predicted the sheer scale for how quickly this area expanded.

In 2019, f-secure [43] claimed to have captured a three-hundred percent increase in traffic attempting to compromise IoT devices since 2018, during just the first half of 2019. This value is one of the last observations of this "normal" exponential growth, as measurements from 2020 became erratic with the development of the Covid-19 situation.

As of 2021, the true effects of the SARS-CoV-2 Coronavirus on IoT based cyber attacks are still not known. Initial results [44, 45] suggest that the gradient in exponential growth of IoT security breaches may have been reduced by lockdowns and work-from-home, as attackers switched to exploit the newly opened attack surface with phishing. Although the rate of acceleration appears to have decreased, the absolute value of breaches is still increasing on an exponent, with Kaspersky's particularly alarming number of 1.5 Billion hits on just their Honeypots. Ipsos MORI (commissioned by the DCMS) additionally found households self-reporting a 57% increase in smart devices in the first six months of the Coronavirus pandemic [45], setting up a potential tremendous expansion as the viability of phishing returns to prior values.

## 2 Contributions

In this paper, a framework is outlined for rapid advancement of the current frontline of Cyber Security in Internet of Things devices. For clarity in the following section, the group of plans, actions and proposals proposed by the United Kingdom Department for Digital Culture Media and Sport will be referred to as the UK Secure by Design Proposal (or simply the UK proposal). The mandate given to ENISA by the European Union, their plans, and their works is referred to as the EU Proposal (Or the ENISA proposal). Within each of these, there is a section of requirements. The UK proposal contains the UK Secure by Design Requirements (UK Requirements) and the ENISA proposal contains the ENISA/EU requirements. This usage of Proposal and Requirements is important to note and remember in this fashion.

The United Kingdom “Secure by Design” proposal was first deconstructed, followed by the parallel ENISA proposal, such that they are expressed in similar fashion. Plan, action and proposal are intertwined extensively in each, and each are also distributed across many different documents. For any further action to be taken, the complete conglomerate proposal of each had to be assembled first, to then be distilled down to simple properties. Any future works can reference these simple well referenced decompositions, and understand both the “Secure by Design” proposal and the ENISA equivalent in respect to each other.

This continues into a targetted deconstruction of the UK requirements expressed in the UK Secure by Design proposal. The initial proposal was rushed to fill a gap post-Brexit, so concerns existed about the suitability of these requirements and whether they were well reasoned. The guidance and justification given for each was examined, with commentary on any possible oversights that may have been made.

The UK requirements were then mapped into the ENISA requirements. Originally this was supposed to be an analysis and joining to create a new superset of requirements better than each individually, however the UK requirements were found to entirely be a subset of the ENISA requirements. As such, it was instead decided to expressly show this superset, and make the links between each UK and ENISA requirement clear, for easy conversion between the two competing standards by future readers. For example, those whom have devices meeting the first UK requirement have now access to corresponding ENISA requirement codes that express that same standard of security. This works the other direction too, with collections of ENISA codes that can map into a UK requirement.

To determine if the UK Proposal with the UK requirements was likely to succeed in it’s stated aims, a semi-random selection of popular IoT devices were taken, and graded (as far as was possible) using the UK Requirements. Based on the stated aims and context given in the UK requirements, if many devices passing was observed it would be an indicator that the requirements were likely to be a bad driver for change. This method yielded many devices passing, indicating the need for an overhaul of these requirements.

Utilising the terminology of the UK Requirements and the specificity of the ENISA requirements, the former were then expanded to entirely include the latter. This resulted in three requirements being added and two UK requirements being dissolved into logical components of other requirements. This, when combined with some of the author’s recommendations, forms a new superset of requirements (referred to as “my own requirements”) and is intended to wholly supersede the UK requirements for any other works on IoT security.

Recognising a favoured proposal from Harris Interactive to create a consumer-facing label building from the original UK Requirements, support and justification for using a point-of-sale label is outlined. However, the potential harm that may be caused by the existing proposal is noted, wherein a poorly developed solution may be more harmful to security than no solution at all. In an effort to cover this eventuality, some “quick-fix” recommendations/alterations are made for the existing solution, which may prevent harm to the cybersecurity ecosystem (primarily, including reference to a date of certification, or a versioning system).

For creating a more comprehensive solution, successes and failures from other relevant areas were analysed. Returning to the basics of label design, the gained insights were used to develop a user-focused prototype for an alternate proposal, without the failings of the existing Harris Interactive label.

Building on the idea that this should be user focused, the prototype is taken to testing with a real-world user study of everyday people. To ensure that higher-level feedback is not neglected, focus groups were hosted for both Cyber Security professionals and Cyber Relevant academics. Specifically attempting to extract information about variables that may not been considered when the label was designed, these all contained significant open-ended segments. From this, good feedback was received for iterating a new label version. Analysing the user study data itself also reveals some interesting trends noted for the future, and used to help interpret focus group answers. The focus groups also feed in additional changes to the design of the label, which when combined with the aforementioned insights from the user studies, further refined the proposed label.

Taking all this feedback, a more refined label is presented along with a concept second-layer (in such a way that it should be compatible with the UK Government style guidelines, such that a true solution with maximal accessibility may be better envisioned). The author of this paper hopes that by taking so any simultaneous steps forward, future works may be able to start from a position far ahead of where they may have previously expected, significantly reducing the timeline for improvements to security in the Internet of Things. Additionally, by laying such a clear emphasis on the end user, future works may continue with this in mind and carry the mindset into circles it may not have previously been prioritised.

## **Part II**

# **Understanding UK IoT “Secure by Design” in a Cybersecurity context**

## **3 Existing Proposals**

### ***3.1 UK Proposal Overview***

Despite repeated assurances that cooperation between the EU and UK would continue in Cyber Security matters [46, 47], in the wake of the 2016 Brexit referendum the Civil Service was tasked with filling the prospective legislative gap that could come from a severing of ties between the two bodies. Prior to this the UK was a partner and contributor towards European Union cybersecurity frameworks, however decided to pursue it's own policy distinct from those organisations after the 2016 referendum [48]. Cooperation in this regard was not negotiated for the withdrawal agreement [49], despite initial recommendations supporting the mandate of ENISA for Cybersecurity [50]. This new UK Cybersecurity framework first manifested as the “Code of Practice for consumer IoT security”, published October 2018 , but drafted March 2018 as part of the Secure by Design report [51]. The rushed necessity of the UK's larger Cyber Strategy has left it open to criticism by the Public Accounts Committee, which concluded in a 2019 report that this approach “lacks the robust evidence base it needs to make informed decisions about cybersecurity” [52].

The Code of Practice for Consumer IoT Security [53] forms the foundation of current-day IoT security proposals, with only minor alterations to the body-text observed throughout the process. It is based on recommendations from a broad range of organisations, but particularly the Internet Security Foundation and ENISA (with its Baseline Security Recommendations for IoT, published November 2017) [54]. This code of practice is outcome-focused, leaving implementation an open question, but makes mention of potential collaborations with retail. Although the recommendations themselves have changed little since first being published in March 2018, there seems to have been a gradual dilution of enforcement. The original draft report states “The Code of Practice is written in priority order, with an indication provided as to which parties each guideline primarily applies to. *The first three guidelines are of particular importance because action in these areas will bring about the largest improvement in security in the short term.*” [51] The latest security requirements and guidance based in this Code of Practice is ETSI EN 303 645 [55], a Baseline Requirements document building from the earlier technical specification. As a formal specification document, recommendation can be distilled from requirement through the use of the keyword “should” as opposed to “will” or “shall” (as per the ETSI drafting rules, section 3.2 [56]). In this document, in the first three requirements with twenty-four subcategories, eleven of them use the optional keyword “should” instead of the mandatory keyword “shall”.

	Requirement 1	Requirement 2	Requirement 3
Should (Optional)		5.2-2, 5.2-3	5.3-1, 5.3-4, 5.3-5, 5.3-6, 5.3-9, 5.3-11, 5.3-12, 5.3-14, 5.3-15
Shall (Mandatory)	5.1-1, 5.1-2, 5.1-3, 5.1-4, 5.1-5	5.2-1	5.3-2, 5.3-3, 5.3-7, 5.3-8, 5.3-10, 5.3-13, 5.3-16

Table 1: ETSI EN 303 645 Mandatory vs Optional wording of First Three Requirements

This analysis is a simplistic and direct method being applied to requirements that can carry substantial nuance, so the author recommends not using this as a baseline for future assumptions and instead visiting the source material to judge it in its entirety. For example, section 5.3 includes “Each provision from 5.3-3 to 5.3-12 is dependent upon an update mechanism being implemented, as per provision 5.3-1 or 5.3-2.” As 5.3-1 is Optional and 5.3-2 Mandatory, to what extent and under what circumstances the Mandatory requirements that follow would apply is unclear in this context. This could result in six mandatory components being avoidable.

	Requirement 1	Requirement 2	Requirement 3
Should (Optional)		4.2-2, 4.2-3	4.3-1, 4.3-2, 4.3-5, 4.3-6, 4.3-7, 4.3-8, 4.3-9
Shall (Mandatory)	4.1-1	4.2-1	4.3-3, 4.3-4

Table 2: ETSI TS 103 645 Mandatory vs Optional wording of First Three Requirements

“IoT products primarily intended to be employed in manufacturing, other industrial applications and healthcare are not in scope of the present document.” - ETSI TS 103 645

In the earlier technical specification [57], there were four “shall” and nine “should”. This initially seems a move forward in security, however the author would again advise that the details in the newer document are important here. A single mandatory point in this older document (4.1-1) has been expanded into five mandatory points in the newer revision, as such the author has concerns that this may in-fact be a regression on enforcement. The focus has been on the first three requirements here, but peering further back in documentation these three requirements were considered simply the priority for short term gains, not the extent of intended coverage [51]. Other potential assistants to raising the baseline of Cyber Security have also been dropped, with a consumer-focused mandatory label proposed by Harris Interactive [58] dropping to voluntary [59], with a promise to revisit the topic in Spring of 2019, and later removed from recommendations altogether over a response to a Call for Views that had just 25 participants [60] (respondents were split three ways on the best approach to labelling).

As ETSI EN 303 645 is the latest work that is building from the Secure by Design heritage, comparison between the original document and this latest revision can provide insight into the current legislative trajectory. For background, this ETSI standard is intended to exceed the “baseline” of Secure by Design, as such readers should consider that devices may be certified as suitable for sale in the UK even if they do not comply with the ETSI requirements. To summarise ETSI EN 303 645 in relation to the original proposal: Only the device itself is within scope, any services or interactions beyond have been placed out-of-scope. Smartphones are not within scope, despite the Department for Culture, Media and Sport explicitly adding them into scope of the UK Secure by Design legislation [61]. The standard is intended to provide a mandatory security baseline, but no more. Recommendations beyond this are made, but these are the same recommendations that have been made since 2014 by many other organisations [38, 39]. The mandatory baseline is in excess of the aforementioned proposals from the UK secure by design proposals in most areas, with some mandatory components in areas declared purely optional by the Secure by Design report. However, the Secure by Design report mandates the first three requirements be mandatory. Of the twenty-four sections covering those first three requirements in the ETSI standard, approximately half are labelled as mandatory (even then, with caveat). This leaves the potential for a device to far exceed the Secure by Design requirements in most areas to comply with ETSI, but leave the device falling short on the essential “core” requirements. How this interaction is handled is a case for the future, as devices are assessed for compliance with both standards. A likely compromise is for ETSI to raise the standard for the first three requirements, or for the UK to declare that meeting those 50% is “good enough” for compliance.

The remainder of the first three requirements, as well as most other content, is retained as guidance and advisement for an organisation which desires to go further. There is no conferred benefit to this action within this proposal (such as being distinguished amongst other devices by the standard), but other schemes are mentioned by name for manufacturers to look into. The text states that the authors expect compliance with this standard will interact in some way with future European legislation. As consumer IoT products become increasingly secure, the authors further elaborate that they envision future revisions of the document will mandate provisions which are currently only recommendations.

### **3.2 EU Proposal Overview**

The EU proposal, when compared to the UK alternative, is a lot less iterative in nature and more comprehensive. The approach of ENISA to tackling large issues seems to be to start from a well defined central concept. Then, once that initial work is completed, dismantle the topic into its component elements which each receive their own specific analysis for their own stakeholders.

For example, the initial well-defined baseline study for securing IoT devices is “Baseline Security Recommendations for IoT”, published 2017 [62]. It includes Eighty-Three requirements and recommendations for improving IoT device security, and it describes itself as aiming to “provide insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures”

In the years following, five additional documents have been released, each targetting a specific subset of IoT devices. Each makes use of that groundwork set in the 2017 paper, and multiple specifically state their purpose is to build on this prior work, with the 2020 paper “Guidelines for Securing the Internet of Things” stating “The IoT threat landscape ... has been analysed exhaustively by ENISA studies that cover the specific elements of the IoT ecosystem. ... This study builds up on existing ENISA studies on IoT security, the baseline IoT security recommendations and the secure software development lifecycle for IoT, and thus should be considered as complementary to the work that has been produced from ENISA the previous years” [63] and the 2021 paper “Good Practices for Security of IoT” stating “...this study tackles one aspect for achieving security by design, a key recommendation that was highlighted in the ENISA Baseline Security Recommendations study” [64]. These works augment the original proposal, such that direct mapping of requirements to subject areas is available for stakeholders, and provide a more high-level overview of the subject. They additionally serve as a more accessible point-of-reference for those in the relevant area, not including materials which would be irrelevant when trying to determine the IoT recommendations that are applicable to a specific area.

As such, in terms of technical content, these additional documents can be regarded as a subset of the original 2017 document. Their primary focus being accessibility, focus, and clarity; they add content only by way of context and explanation. While valuable to the stakeholders the documents were designed for, they add no technical insight when viewing the whole scope of IoT devices from a recommendations perspective, and will subsequently be excluded from analysis.

These works by ENISA are initiated by directives from the EU (or by specific request of a member state), and as such their works and publications are often processed and encoded into law by the EU. This approach of the security policy being commissioned by the legislature and then enforcing what returns onto member states gives recommendations from ENISA a lot of “weight” behind them, such that it can be difficult to ignore them for long. The EU Cybersecurity strategy was proposed by the European Commission in 2013 [65] and supported with a legal directive three years later [66] referred to as NIS (Network of Information and Systems). ENISA was then given a mandate to support this directive which resulted in the 2017 Baseline Requirements for IoT. This fed back into the Commission, which resulted in new initiatives, proposals and a specific proposal “for a stronger mandate for ENISA, so that it can become a true EU Cybersecurity agency” [67]. This proposal was approved in 2019 [68] and a subsequent directive for ENISA nicknamed “NIS2” has been proposed [69], which is one full cycle of the iterative process used by the European Commission. As the citations show, it can take some time for this cycle to complete, but the reliability of recommendations making their way into legislature is what gives ENISA recommendations such legitimacy and power.

## 4 Relevant Works to understanding the Cybersecurity context

Looking closer into the current IoT landscape, it became clear that there is strong support and justification for a system to improve availability and accessibility of information to consumers. The report “What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?” [70] works to analyse the current information available to the consumer through trawling product-adjacent online content, including manuals. It highlights the poor state of communication to consumers, as even if they were to read the complete manual, most information is missing. This is unsurprising, as trying to explain a concept of encryption and how it protects a user would be exceedingly challenging. The report argues for “government intervention in this space to provide assurances around device security”. This concept of providing reassurance is something intended to bring in-scope to the works outlined in this paper, as an important quality beyond just providing information. Some success stories for communication can be seen within the NCSC and their Cyber Aware program. Information is clearly conveyed in few words, with deeper explanation only if the user desires it [71].

The results of this study which informed that author’s strong stance are (based on this author’s own classification of existing devices) likely to be low estimates, due to their listed methodology. When determining if a device will be certified as meeting a requirement (example: requirement two, have a vulnerability disclosure policy) the methodology listed is to search using the query [‘Device name’ AND ‘security’ or ‘encryption’ or ‘password’ or ‘updates’ or ‘vulnerability disclosure’]. This will bring up few positive results, as information can be dictated on the company level and inherited by all products. In the example of Requirement Two, vulnerability disclosure policies are usually listed as a singular policy for the manufacturer, not on each product page. Were the search to even expand to a more spider-like “search the entire domain for a vulnerability disclose policy”, many brand-name companies are actually subsidiaries of larger organisations and as such have the policy dictated on the higher domain (for example, Nest being part of Google and Alphabet inherits the Alphabet Vulnerability Disclose Policy, hosted on a Google domain). The study concludes that the information provided through manuals and support pages is inadequate, with recommendations to store security information in a centralised repository and to find a way to communicate device security in a more accessible format, outright recommending a labelling scheme.

This support of a labelling scheme is a common theme in recent literature. Blythe 2018 [72] provides a report that outlines the successes of previous labelling schemes and makes the case that a similar approach could be taken for IoT devices, with the intention to rectify information asymmetry between the consumer, retailer and manufacturer. Through analysis of labels in other industries, the report recommends that “the choice of the most appropriate format of the labelling scheme needs to be evidence based and derived from research on consumer behaviour and subsequent consumer testing”. The three broad observations about what makes a successful label that are observed in other studies are that Colour Grading Schemes are the most preferred option, but that companies may be unwilling to subscribe to this implementation without it being mandatory. A binary “approved or not-approved” is simpler and likely to be adopted even without being mandatory, but it has the potential to lead consumers into a false sense of security and are less effective for their intended purpose of informing consumer choice. Lastly, that a descriptive information-only label (while potentially an adequate way to communicate the most important information to consumers) would have to undergo significant user testing. Specifically, issues were observed with misunderstanding symbols in the EU Energy Labels and consumers were giving weight to certain types of information in a manner that lead to biased search behaviour [73].

Following this, there are moves by the DCMS to improve device security in Britain. As such, they began commissioning reports on the current IoT landscape (such as the PETRAS Literature Review [54]), as well as potential strategies to tackle the issues. One particular report of interest is “Consumer Internet of Things Security Labelling” [58]. Harris Interactive were commissioned by the DCMS to analyse four draft label designs, such that the best design for informing the public about safety and security features for IoT devices could be determined. The direct cause for investigation was “to investigate both the effectiveness of the labels and potential premium pricing for label-carrying products”. Harris Interactive weighted a total sample of 6,482 usable responses by the census data for ages 16+ and distributed these blindly across both the four label designs and four different smart devices, allowing testing of devices with each label. The resulting distribution of participants is displayed in Figure 4, created by Harris Interactive as part of the report.




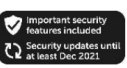
	<b>Shield with Text Underneath</b> 	<b>Shield with Text Inside</b> 	<b>Icons with Text Underneath</b> 	<b>Full Lozenge</b> 
<b>Label Abbreviation</b>	<b>Label 1</b>	<b>Label 2</b>	<b>Label 3</b>	<b>Label 4</b>
Smart TV	404	405	412	406
Wearable Device	403	407	403	409
Smart Toy	405	406	403	403
Smart Thermostat	404	402	407	403

Figure 4: The participant distribution for a survey performed by Harris Interactive. Four labels were tested (labels 1 through 4) and four different mock-devices were tested. These are a “smart TV”, “Wearable device”, “smart toy” and “smart thermostat”. Within, it can be seen that around four hundred participants were exposed to each combination for label and device. Specifically, the lowest value is 402 participants, whilst the highest is 409. [58]

Lots of useful data was gathered during this survey around consumer expectations and intentions with their devices, and a clear superior label design of the four presented was determined. However, the report was commissioned with a price-point premium in mind rather than label effectiveness as their primary concern. Although an interesting question whether price-point premium is the correct way to design a label, we leave that question for device manufacturers and adopting companies to contemplate.

Additionally, only the four provided labels were able to be considered, with no opportunity to test variation of the messaging system. The label design which Harris Interactive concludes to be the best choice will be used during the author’s own works as the “mark to beat” for the criteria that both independent research and the DCMS have identified as priority.



This need for IoT device labelling has also not gone unnoticed in academia, with a study from Carnegie Mellon University running in parallel to this author's own. "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" [74] is a report that is intended to complement efforts by legislators to incorporate labels for security purposes, by analysing expert opinions on priority factors in conveying security risk to consumers. The report supports a label which conveys advanced features, promoting competition and differentiation between companies. A prototype design is demonstrated at the end of the report, which is intended to show the findings and recommendations from their studies in a visual manner. "Based on the results of our expert elicitation and consumer studies, we propose a prototype privacy and security label to help consumers make more informed IoT-related purchase decisions." However, this prototype label contains many unworkable information displays and sources of confusion. By including printed-on firmware versions and date of last update, this disincentivises updates to any stored stock that has already left the factory, as product packaging would have to be replaced. Additionally, many fields can be rendered out-of-date immediately. As seen with the ESRB game ratings for "In-Game Purchases", printing on-box negatives is ineffective. Many games leave the factory for rating as "no in-game purchases", but will update themselves to include such features after receiving the label [75]. This can be avoided by providing information of what a product does include or operate with, rather than what it does not do. While possible to still move backwards and lose features with patches, little incentive is provided for such evasion by device manufacturers, due to the cost of feature implementation already being paid. The two-layer label also relies on a QR code for transfer from the physical label to the more detailed online component.

#### **4.1 A note on QR Codes**

A recurring feature or request by many researchers is for a QR code to feature on consumer packaging and be integrated into any proposal for a two-layer system. In 2020, the Office for National Statistics recorded 16% of the population do not have a smartphone for private use [76]. However, of particular note is that this ONS data was collected via online survey, and as such will have results biased towards those with smart-device competency. Statistics around recognition of QR codes are not up-to-date (it is expected that reach should broaden year on year with greater market penetration, so old statistics could be misleading) however Harris Interactive explored the concept in 2019 when making design decisions around their own label [58]. With a representative sample of UK demographics (however still polled online) 46% of participants were identified as not knowing how to scan a QR code. It would be inappropriate to exclude (at least) 16% of the population, especially when that figure is likely to contain those most in-need of guidance around smart devices. Any adopted method of reaching more information should include instructions for operation, and be accessible without any specific device prerequisite. The UK Government had guidance it provides to its public sector bodies for this topic, under "Assisted Digital Support" [77, 78, 79]. Since these bodies also have the same target, of being accessible to all the UK populace, their guidance has been kept in mind when choosing to exclude QR codes and instead adopt a more supportable method of accessing online information.

## 5 Existing Proposal Analysis and Deconstruction

### 5.1 Analysis of UK IoT “Secure by Design” Requirements

For a deeper analysis of the UK Government proposal, the prior materials used to justify the choices made have been examined. It should be noted that there are many silent revisions of these 13 requirements, with sources appearing and disappearing along with accompanying text. The existence of these revisions at all was only noticed due stringent author record-keeping, and there is no indication given by the DCMS that a source document has been altered since it’s initial upload. It is possible an update may have silently occurred during a single period of analysis, as such minor inconsistencies may be observed between recurring analysis of the same materials. The only listed document preceding the draft review is the PETRAS Literature Review [54], however it should be noted that there are still other sources, just listed internally to the document and standard instead of externally. The PETRAS Review’s stated objectives are to “identify the key themes emerging from the literature and identify international consensus around core Security by Design principles for the IoT”, and the paper author wishes to firstly remark that this seems ill-fitting for background research into creating a foundation for security. To expand this critical analysis, the most immediate oddity upon reading this document is that occurrences were only counted to inform the literature review, not analysed. By this, it is meant that when determining what requirements would be passed forward into creating the Secure by Design standard, no analysis beyond “How often do people mention X?” is performed. This is due to the keyword “Identify” being used during those objectives. Were the data truly enormous, such stripping of analysis may be justified, however such a weak determination of importance headlining as the sole listed justification for requirement choices is concerning. Unfortunately, a true critical analysis of this work and it’s methodology is beyond the scope of this document, so the decisions made during (and around) the PETRAS literature review are left to the reader to interpret.

When reviewing how this counting of occurrences is processed into a requirement, there is a mapping within the document that can be reviewed. The Mapping provided simply lists all the occurrences, and quotes the exact point the authors found it. This results in a “fuzzing” of the guidance from the source documents, where rather than the guidance directly informing a requirement, it instead goes through a counting screen that strips it of context before requirements worth acting on are chosen.

Were these proposals scrapped and the project started again, the subjective opinion of this researcher is that the guidance gathered by PETRAS is of good quality, and could form a significant foundation of successor works. The largest single reason for the shortcomings in the PETRAS report is the stripping down of the quality guidance, which is a fault easily remedied. Reducing dimensionality of data is an essential part of analysis, but reducing each report to just a binary bit representing ‘if a topic is mentioned’ appears to have harmed the integrity of the proposal. A stronger link between each recommendation and the requirements they inform would make it clear which advice has been deliberately rejected due to being unsuitable, as opposed to which guidance was simply overlooked.

#### 1. No default passwords

“All IoT device passwords shall be unique and not resettable to any universal factory default value.”

“Many IoT devices are being sold with universal default usernames and passwords (such as “admin, admin”) which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed. Further details are available on the NCSC website.

<https://www.ncsc.gov.uk/guidance>”

Devices should ship with unique default usernames and passwords. They must also not be resettable to any non-unique pairs (for example, those used in factory testing). No mention is made about including no password as a default.

Advice to the government for this section has come from the NCSC [80] and NIST [81]. The recommendation defends against few of the attacks mentioned in both reports. Given that the government intends to take a secure by design approach, whereas the guidance given is more user focused, it is unsurprising that they do not line up well. However, this author would have expected a secure by design approach to prevent these user security issues from arising when implemented correctly. Instead, the author finds little would change for end user security requirements if the government's guidance were followed. For example, of the six recommendations made by the NCSC to improve system security, the government recommendations do not address or attempt to address the risks posed by any. All would still occur on devices certified as meeting the government's password requirements.

Although a good policy in isolation, a secure by design approach has the ability to take security here further with little extra effort or cost from device manufacturers. If sensible password minimum requirements were also included here (or sensible password alternatives allowed as a substitute) along with a statement about lockouts for incorrect passwords, roughly half of the NCSC recommendations for improving system security would no longer be necessary for IoT devices. Further recommendations can be rendered moot if some helpful guidance were included with the device, specifically regarding password choice. Since IoT devices always have an internet connection, checking against a centrally stored database of common and frequently compromised password hashes would be an easy improvement that can further enhance security, adding enhanced defence against dictionary attacks and rainbow tables.

#### Implement a vulnerability disclosure policy

“All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.”

“Knowing about a security vulnerability allows companies to respond. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Reports of vulnerabilities can be sent to: [security@ncsc.gov.uk](mailto:security@ncsc.gov.uk). Companies are also encouraged to share information with competent industry bodies. Competent industry bodies include the GSMA and the IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure is available from the IoT Security Foundation which references the ISO/IEC 29147 standard on vulnerability disclosure. The GSMA's industry level Coordinated Vulnerability Disclosure programme is located at: <https://www.gsma.com/cvd>”

A mandatory point of contact for vulnerability disclosure leaves a paper trail on any disclosed vulnerabilities. Previously, many companies have had no mechanism for reports and have been able to simply ignore any they receive, pleading ignorance upon investigation. Although no hard limits are imposed, the requirement does state the de facto standard for a patch is no longer than 90 days.

The government has modelled this after the GSMA's coordinated vulnerability disclosure policy [82], which is held as an example of how to conduct vulnerability disclosure correctly. Additionally, reference is made to ISO/IEC 29147 [83]. However, the recommendation in the report seems to only superficially resemble the guidance they have been given, and indeed the guidance they are giving out for what responsible disclosure looks like.

For example, the GSMA importantly includes guarantees for the reporter of a vulnerability which are crucial for the system to work. Reports are treated confidentially or can be given anonymously, credit for vulnerabilities is offered and a guarantee of responding within ten working days is given. ISO/IEC 29147:2018 has been withdrawn by the time of this document.

There would be no extra cost associated with adding these amendments to the proposal, their existence would simply reinforce the intended use of this requirement. There have been many cases where those reporting bugs are punished rather than praised for their finds, even by large companies [84, 85]. Including protections for those reporting issues in the requirement will foster an environment where disclosers can feel confident in reporting their findings directly to a company, which seems to have been the original intent of this requirement.

#### Keep software updated

“Software components in internet-connected devices should be securely updatable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.”

“Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support must be made clear to a consumer when purchasing the product. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.”

Updates should be delivered in a secure manner as to prevent delivery of malicious software upgrades. No information is given on whether updates should be mandatory, the possibility of “kill the device” updates is also left open for arguments of security (to prevent a device from being used once it is no longer secure, versus to force a replacement purchase). Additionally, there is a non-mandatory request for the device to remain functioning during an update.

Guidance for this requirement is not included with the document (or any subsequent requirement), so the PETRAS literature review that informed these requirements will be relied upon. This requirement largely corresponds with the guidance given, with just a few recommendations not being implemented. These are that devices should ship with the most up-to-date stable version, that updates be thoroughly test, that devices have a fallback/rollback option and that devices use signatures to verify the updates are from a trusted source.

No guidelines are laid out for timely deployment of updates, meaning interpretation of this law will be decided in the courts. Additionally, as mentioned there is no consideration for user choice in this guideline. Are all updates now mandatory? Or are only security updates mandatory? What if security updates are bundled with anti-features? Apple and Samsung were found guilty of shipping updates that slowed older devices, with the accusation that this was a deliberate choice to encourage the purchase of new phones [86], a practice that IoT devices may similarly be vulnerable to.

Devices remaining functional during updates removes the possibility of resetting to safe states, and would not be possible for firmware updates. An alternative proposal is that devices should indicate to the end user when they are resetting for an update, with some communication provided for how long the system will likely be inoperable. Removing the recommended “fallback/rollback” option for updates leaves devices vulnerable to updates which unintentionally damage the device, as was the case with an AMD driver update in 2015 [87, 88]

#### Securely store credentials and security-sensitive data

“Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.”

“Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment and associated trusted, secure storage. Stored credentials in services should follow best practices.  
<https://pages.nist.gov/800-63-3/sp800-63b.html#sec5>”

Outside of credentials, examples of security-sensitive data can include cryptographic keys, device identifiers and initialisation vectors. “Securely store” does not give any indication of what an implementation may look like, or any specific recommendations for those looking to meet this requirement. In the PETRAS literature review, the only point that seems to correspond to this requirement is that “Salt, hash and/or encrypt credentials”. Elaborating on this further using the OWASP recommendations [89], hashing the password should be one of several steps (to prevent DOS through long passwords, or truncating lengthy passwords) and the salt should be cryptographically-strong. Encryption through adaptive one-way functions or keyed functions are both recommended.

Addition factors which should be considered are that even if credentials are kept in a secure medium, they should be stored assuming the medium will eventually be compromised. If the storage medium relies on being inaccessible for security, then the storage medium is only as strong as it’s secrecy, and security through obscurity is no security at all. Relying on a third-party solution for securely storing keys (for example, Google’s project Vault) leaves all devices of a kind vulnerable once that third-party is compromised, with no avenue to simply reissue new keys.

The primary challenge with securing encryption keys for IoT devices is that, as they are a single device, keys will always be stored in the same location as the data they decrypt. Integrating sub-processors to act as a “separate machine” that can store the keys are one possible option, but this may not always be possible and provides additional attack surfaces that may be exploited [90] (see requirement six for additional information on the importance of reducing attack surfaces).

#### Communicate securely

“Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.”

“The use of open, peer-reviewed internet standards is strongly encouraged.”

This requirement is unfortunately vague. Traffic encryption will prevent MITM attacks which could compromise privacy, device functionality and more. Any attempt to clarify further on encryption quality for standards could unintentionally exclude low power devices, and attempting to compensate can leave poor implementations on high-power devices open to still matching the requirement. The PETRAS literature review conducted to support the report is similarly vague, with no dedicated category and simply a “Use best practice cryptography protocols” justifying this requirement.

The NCSC guidance on this topic is far more clear on what would constitute secure, providing details on what would constitute good practice with regards to TLS and being clear about how devices should handle their connections through the internet [91]. The provided information was out of date, however, not including any information on TLS 1.3 until (if their self-declared publication dates are correct) three years after 1.3 first began deployment.

While not specifying specific cryptographic protocols is good for a requirement, lest they are unsuitable for a device or are compromised, this requirement is currently too vague for any company to comply with. Specifying an “average compute hours to crack, for currentYear computers” requirement would go a long way to fleshing out this requirement, having the advantage of increasing in difficulty automatically each year to correspond with advances in both cryptographic cracking algorithms and computer architecture. While it does not solve the issue of low power devices that cannot realistically provide cryptographically secure encryption for real-time traffic being unable to meet the requirement, attempting to lower the bar such that they can compete would compromise the integrity of the entire requirement. Advances are still being made in the field of low-power encryption [92], so the exclusion of these devices may be regarded as only temporary until the field catches up.

#### Minimise exposed attack surfaces

“All devices and services should operate on the ‘principle of least privilege’; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.”

“The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.”

An often over-looked aspect of reducing attack surfaces in cybersecurity is to secure not only internet-facing attack surfaces and physical access points, but also local area threats. With the range of 802.11n setting the current realistic max range of around 100 metres for each device [93] and the increased emphasis on mesh-networks for 802.11ax [94], a weak-link device on the internal network could potentially compromise other local area devices, even outside the current premises. The literature review accompanying the report further elaborates on how some controls could be implemented, disabling connectivity or ports which are unnecessary for the core product functionality.

Little mention is made within the literature review of this important requirement, with a single point being “Build in controls to disable connectivity or disable ports to mitigate potential threats, while maintaining core product functionality” covering the scope and intention of this requirement.

This recommendation is broad and sweeping, but conveys its intent well. Having controls to disable surfaces which are surplus to requirement is a good step, but still leaves the burden on the user to know both what to disable and how to do it. One improvement may be to include some pre-set behaviours tailored to some expected use cases of the product. An example of this which has seen great success is the network security settings for Microsoft Windows. As Windows has such a broad user-base with customers using the same product for home as well as commercial applications, when first connecting to a new network a prompt will appear with three different presets suitable for different use cases (along with a short description of each, so the customer can easily identify which category they fall into). Prompts with different presets would be easily implemented for most IoT devices, with possible additional settings than “work” and “public” being related to the network in the home (connected directly to the internet, connected to another IoT device, connected to a router) or how the user intends to utilise the device (keep my data only on this device, allow my data to be communicated to other specified devices on the local network with an authorised key, allow my data to be accessible from the internet through an API) helping ensure that the device is properly configured for the use case the customer needs.

#### Ensure software integrity

“Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.”

“The ability to remotely recover from these situations should rely on a known good state, such as locally storing a known good version to enable safe recovery and updating of the device. This will avoid denial of service and costly recalls or maintenance visits, whilst managing the risk of potential takeover of the device by an attacker subverting update or other network communications mechanisms.”

Reverting to a known “safe” version is a good strategy but a vulnerability all in itself. If release 1.0 is compromised and patched, resetting a device can be a tactic to gain control of a device. The requirement additionally elaborates on this avoiding denial of service (when a large number of devices are taken offline, then reconnecting to host servers all at once can cause a ripple of denial of service. See requirement nine.), but this seems to imply that an order can be given to reset devices back to the 1.0 software remotely in case of widespread compromise. In addition to the included requirements, the literature review conducted by PETRAS also identified some additional features which could be integrated with a Reset mechanism. They seem to be focused around providing a customer and the manufacturer with the tools they need to both determine when a Reset would be needed, and providing support to the customer during the process. Given that the additional support to the customer would require a phone line or other manned support line (and would therefore incur a non-trivial cost) it is unsurprising but disappointing that it was omitted from the requirements. It provided significant benefits for removing the burden of security from the consumer and back onto the manufacturer, one of the stated goals of these requirements, but additional works commissioned by the DCMS included cost as a primary concern [58]. The suggestion of making Secure Boot mandatory would likely also face legal challenge from consumer advocacy groups, especially with the manufacturer retaining the ability to reset their devices remotely.

Ensure that personal data is protected

“Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers’ consent, this shall be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.”

“This guideline ensures that:

- i. IoT manufacturers, service providers and application developers adhere to data protection obligations when developing and delivering products and services;
- ii. Personal data is processed in accordance with data protection law;
- iii. Users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified;
- iv. Users are provided with means to preserve their privacy by configuring device and service functionality appropriately.”

Within the literature review, the issue(s) of privacy are raised frequently, often with regard to the GDPR. Excluding GDPR related recommendations, disclosure of what happens to data when ownership is transferred of a device, providing a user with the option to delete personal data on company services when ending service with the company (and control personal data at any point of the lifecycle, including choices about what data is collected) and that consent has to be granted for personal data to be shared with third parties are all included.

Although security and privacy often cover similar ground, they are distinct topics. This requirement is a more privacy focused point, seemingly included to bring the GDPR in-scope. The recommendations beyond the GDPR are largely lost from the requirement.

Make systems resilient to outages

“Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.”

“IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures may include building redundancy into services as well as mitigations against DDoS attacks. The level of resilience necessary should be proportionate and determined by usage but consideration should be given to others that may rely on the system, service or device as there may be a wider impact than expected.”

Of particular note is the “rather than in a massive scale reconnect”, which is intended to stop ripples of high demand following a service interruption which could themselves cause further interruptions simulating a DDOS attack. As IoT devices are expected to be integrated further into everyday life, it is reasonable to expect they can either continue functioning if they serve a critical role even if they receive an update. An interruption to a device controlling the electricity supply, for example, could cause a chain reaction of other failures (which may even be life threatening). An interruption to an IoT door lock is another scenario that highlights why simply resetting the device when it updates may not be an option. If the device simply reset, either a customer could be locked out of their home while their device updates or there may be no locking at all.

There is little to add to this requirement, except to emphasise the difficulty of what is being asked and how this could unintentionally leave devices in a more compromised and hard to troubleshoot position. In terms of verification, if you have identified that there exists a compromised or otherwise faulty state (or set of states) Y which exhibit unexpected behaviour, then without a reset to a “safe state” of intended behaviour (X) you cannot guarantee any patch will not leave the machine still in that compromised state (either the same Y, or an entirely new Z introduced through this effort to escape Y). This difficulty is why most devices choose to reset to apply updates, to ensure that the state of the machine is within the domain that defines the bound of expected behaviours when an update is applied.

#### Monitor system telemetry data

“If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.”

“Monitoring telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimising security risk and allowing quick mitigation of problems. In accordance with Guideline Eight, however, the processing of personal data should be kept to a minimum and consumers shall be provided with information on what data is collected and the reasons for this.”

This rule puts a responsibility to companies collecting this extra data to provide some benefit back to the consumers. It may provide justification for extraneous data collection, however.

This rule contradicts some recommendations made in the literature review, which is a contradiction acknowledged by the requirement, and states that personal data should be avoided where possible to prevent clashing with requirement eight. The literature review goes further than this though, stating “Design to collect only the minimum amount of data necessary”, while the requirement has the keyword “Personal” added as a modifier. Additionally, another section of the literature review mentions providing choices for data collection beyond what is necessary for device operation. Generally speaking, the literature review seems to favour consumer choice and freedom while the proposed requirements provide more lax restrictions for companies collecting data.



Collection of system diagnostic data is useful for companies looking to improve their product. However, it cannot be ignored that the users receive little benefit for providing this information. Providing a mandate that 'if the data is collected, it must be used to provide a security benefit to the consumer' is a large step forward in this regard, however the "Personal" keyword modifier should be removed, returning to the suggested version. The original recommendation's additions should be retained, to help keep this requirement in-line with the message of both requirement eight and the GDPR.

#### Make it easy for consumers to delete personal data

"Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data."

"IoT devices may change ownership and will eventually be recycled or disposed of. Mechanisms can be provided that allow the consumer to remain in control and remove personal data from services, devices and applications."

Given the nature of IoT devices to be tightly intertwined with data collection and the internet, a way to control this data in case of disposal or resale is necessary.

The literature review provides a request for a mechanism to reset to the manufacturer state, just as it appears in the requirement, but makes further recommendations with respect to user data, including that companies disclose what happens to user data when ownership is transferred. This mechanism is unfortunately omitted from the DCMS proposal. The importance of including a way of securely wiping data is highlighted in the justification for a security label [58], where Harris Interactive reveal that the most common methods of device disposal leave data left on a device open to exploitation.

Even the literature review recommendations do not go far enough for this requirement. Although a factory reset is perceived as a way of securely removing personal data, this is not the case. Recovery of data on Android devices, for example, is not only possible but trivial [95]. This shortcoming is especially notable as mobile devices will have similar power constraints to IoT devices. A better practice for wiping data will be to first encrypt the device volume before wiping it. This drastically reduces the risk of leaking sensitive data, as any information which can be recovered will be useless without the decryption key. Even that can not be enough, however, as mobile devices in particular tend to use short decryption keys for ease of input, which opens them to brute force attacks [95]. Given the interfaces for IoT devices tend to be similarly compact, it is not unreasonable to expect that similar decisions regarding password length could be made.

#### Make installation and maintenance of devices easy

"Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device."

"Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats."

Where a secure-by-design approach cannot give security, devices should be hard to misconfigure. Some good steps to this would be "recommended" safe options for standard users, with other options being labelled for advanced users. Maintenance is less clear.

No guidance in the literature review lines up particularly well with this requirement, it is more implied through the implementation of other requirements. For example, "Provide controls to edit privacy settings" would be of little use without also making sure these controls are easy to use, with minimal steps and best practice for usability.

Implementing a set of recommended common configurations, as mentioned in the suggestions for requirement six, would go a long way to help users with the installation of their devices. Prompts for recommended maintenance actions (“your device is a running a little slow, here are a few actions which could help speed it back up”) would expand on this existing user experience, promoting an environment where the burden of knowledge is lessened for the end user and they instead are relying more on quality recommendations for their circumstance. This does bring a danger of bad recommendations souring the user experience, so care should be taken to ensure that if a manufacturer is going to include recommendations that they aspire to meet the expectation of quality from the end users.

#### Validate input data

“Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.”

“Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

- i) Not of the expected type, for example executable code rather than user inputted text.
- ii) Out of range, for example a temperature value which is beyond the limits of a sensor.”

More “Software Design” than anything specifically related to IoT devices, attention should be paid to the dangers of values outside expected parameters. No safe values should be presumed, especially when working with other devices, else errors could cascade throughout an entire network of devices from a single bad sensor.

Like the previous requirement, this requirement is more implied by other recommendations. The recommendation of “Undergo a secure development process”, for example, would flag lack of validation of input data as a serious issue.

The narrowing of scope from the general “Undergo a secure development process (such as threat modelling, inventory of codes)” to just validating input data has changed a robust requirement which only the best of devices would be able to meet into a low floor. Any company with even the most modest of knowledge of good coding practice would be able to meet such a requirement. While this easy-to-meet requirement is good for stakeholders who want to make meeting these security requirements as simple as possible, it indirectly harms companies who have an interest in securing their devices as strongly as possible, as there is no longer an incentive to push for the high ceiling. By providing no consumer communicable method of differentiating themselves in the market, they have removed a major benefit for companies who have a desire to make security on their devices as robust as possible. This is especially problematic for industry, where a true Secure by Design supply chain has long been recommended [63].

## **5.2 Mapping UK IoT “Secure by Design” into ENISA Baseline Security Requirements for IoT**

As mentioned in subsection 3.2, the EU requirements are (collectively) far more comprehensive when compared to the UK requirements, and wholly encompass the UK proposal (Demonstrated below). With eighty-three specifically focused objectives that can be treated as a “checklist”, they are each clearly worded such that there is as little room for interpretation as possible. Consequently, when trying to suggest wording alterations to any specific requirement, their absolute specificity and clear meaning left naught to improve. Each individual requirement is given a code (for example, GP-TM-09) such that they can easily be referred to, which I will also use here.

To prove the UK requirements are wholly a subset of the EU requirements, extended features drawn from EU requirements have also been included rather than strictly aiming for parity. There is additionally some crossover in categories, where some requirements can logically be deconstructed into components of other categories without effecting the coverage. This emerges when incorporating EU requirements related to the subject area but that are considerably beyond the limited UK requirements. These are included under a “Additional related elements” label, such that a reader can reason the dissolution of UK requirements 11 and 12 while still maintaining the statement that the UK requirements are a subset.

For a more visual proof, Table 3 expresses this mapping (subsection 5.2) as a table.

## 1. *No default passwords*

### *Stated UK Requirement*

All IoT device passwords must be unique and not resettable to any universal factory default value.

Many IoT devices are being sold with universal default usernames and passwords (such as ‘admin, admin’) which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed. Further details are available on the NCSC website.

<https://www.ncsc.gov.uk/collection/passwordshttps://pages.nist.gov/800-63-3/sp800-63b.html#sec5>

### *EU Requirement Mapping:*

GP-TM-09: Establish hard to crack device individual default passwords. Usernames and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked, and a hard to crack default password is still a weakness if it is used for more than one device.

GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.

GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates.

### *Additional related elements:*

GP-TM-25: Protect against ‘brute force’ and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts, or by making the user wait a certain amount of time to login again after a failed attempt. This protection should also consider keys stored in devices.

GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.

## 2. *Implement a vulnerability disclosure policy*

### *Stated UK Requirement*

All companies that provide internet-connected devices and services must provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

Knowing about a security vulnerability allows companies to respond. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Vulnerabilities should be reported directly to the affected stakeholders in the first instance. If that is not possible vulnerabilities may be reported to national authorities

<https://www.ncsc.gov.uk/contact>. Further details of the different approaches to take in different circumstances are included in the explanatory notes. Companies are also encouraged to share information with competent industry bodies <https://www.gsma.com/cvd>

#### *EU Requirement Mapping:*

GP-OP-06: Coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT).

GP-OP-07: Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.

GP-OP-08: Create a publicly disclosed mechanism for vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.

#### *Additional related elements:*

GP-PS-06: For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.

GP-TM-57: The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches. Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.

### 3. *Keep software updated*

#### *Stated UK Requirement*

Software components in internet-connected devices should be securely updatable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

The provenance of security patches should also be assured and they should be delivered over a secure channel. The basic functions of a device should continue to operate during an update wherever possible, for example a watch should continue to tell the time, a home thermostat should still operate and a lock should continue to unlock and lock. This may seem primarily a design consideration, but can become a critical safety issue for some types of devices and systems if not considered or managed correctly.

Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support shall be made clear to a consumer when purchasing the product. The retailer and/or manufacturers should inform the consumer that an update is required. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.

*EU Requirement Mapping:*

GP-OP-01: Develop an end-of-life strategy for IoT products. Security patches and updates will eventually be discontinued for some IoT devices. Therefore, developers should prepare and communicate a product sunset plan from the initial stages to ensure that manufacturers and consumers are aware of the risks posed to a device beyond its expected expiry date.

GP-OP-02: Disclose the duration and end-of-life security and patch support (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase.

GP-TM-18: Ensure the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins. Failing to build in OTA update capabilities will leave devices exposed to threats and vulnerabilities for the entirety of their lifetimes.

GP-OP-03: Monitor the performance and patch known vulnerabilities up until the “end-of-support—” period of a product’s lifecycle. Due to the limited life cycle of many IoT devices, critical, publicly known security or privacy bugs will pose a risk to consumers using outdated devices.

4. *Securely store credentials and security-sensitive data*

*Stated UK Requirement*

Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.

Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys, device identifiers and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment and associated trusted, secure storage.

*EU Requirement Mapping:*

GP-TM-24: Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.

GP-TM-35: Cryptographic keys must be securely managed. Encryption is only as robust as the ability for any encryption based system to keep the encryption key hidden. Cryptographic key management includes key generation, distribution, storage, and maintenance.

GP-TM-49: Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.

5. *Communicate securely*

*Stated UK Requirement*

Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.

The use of open, peer-reviewed internet standards is strongly encouraged.

*EU Requirement Mapping:*

GP-TM-34: Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.

GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.

*Additional related elements:*

GP-TM-07: Use protocols and mechanisms able to represent and manage trust and trust relationships. Each communication channel must be trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions).

GP-TM-36: Build devices to be compatible with lightweight encryption and security techniques (including entities secure identification, secure configuration, etc.) that can, on the one hand, be usable on resource-constrained devices, and, on the other hand, be scalable so to minimise the management effort and maximise their usability.

GP-TM-37: Support scalable key management schemes. It has to be considered that tiny sensor nodes cannot provide all security features because they have lots of system limitations. Thus, the sensed data carried over infrastructure networks may not have strong encryption or security protection.

GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.

GP-TM-41: Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways). Data is often stored, cached, and processed by several nodes; not just sent from point A to point B. For these reasons, data should always be signed whenever and wherever the data is captured and stored.

GP-TM-52: Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.

GP-OP-04: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided. Purely proprietary approaches and standards limit interoperability and can severely hamper the potential of the Digital Single Market. Common open standards will help users access new innovative services, especially for SMEs, the public sector and the scientific community. In particular, the portability of applications and data between different providers is essential to avoid lock-in.

6. *Minimise exposed attack surfaces*

*Stated UK Requirement*

All devices and services should operate on the 'principle of least privilege'; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

*EU Requirement Mapping:*

GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.

GP-TM-50: Ensure only necessary ports are exposed and available.

GP-TM-08: Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default. Strong security controls should be something the consumer has to deliberately disable rather than deliberately enable.

GP-TM-43: IoT devices should be restrictive rather than permissive in communicating: When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.

GP-TM-45: Disable specific ports and/or network connections for selective connectivity. If necessary, provide users with guidelines to perform this process in the final implementation.

GP-PS-12: Identify the intended use and environment of a given IoT device. This will help developers and manufacturers determine the most suitable technical features for the IoT device's operation, and the security measures required. This will also help to effectively handle bugs or enhancement requests.

*Additional related elements:*

GP-TM-30: Ensure a context-based security and privacy that reflects different levels of importance (e.g. emergency crisis, home automation).

7. *Ensure software integrity*

*Stated UK Requirement*

Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

The ability to remotely recover from these situations should rely on a known good state, such as locally storing a known good version to enable safe recovery and updating of the device. This will avoid denial of service and costly recalls or maintenance visits, whilst managing the risk of potential takeover of the device by an attacker subverting update or other network communications mechanisms.

*EU Requirement Mapping:*

GP-TM-03: The boot process initialises the main hardware components, and starts the operating system. Trust must be established in the boot environment before any trust in any other software or executable program can be claimed, so the booted environment must be verified and determined to be in an uncompromised state.

GP-TM-04: Sign code cryptographically to ensure it has not been tampered with after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded. Only run signed code and never unsigned code. Measuring the boot process enables the detection of manipulation of the host OS and software, so that malicious changes in the behaviour of the devices can be detected. It enables boot-time detection of rootkits, viruses and worms.

GP-TM-06: Restore Secure State - Enable a system to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful.

*Additional related elements:*

GP-TM-01: Employ a hardware-based immutable root of trust. The Hardware Root of Trust is a trusted hardware component which receives control at power-on. It then extends the chain of trust to other hardware, firmware, and software components. The Root of Trust should then be attestable by software agents running within and throughout the infrastructure.

GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, that provide:

- Chain of trust boot-loader which authenticates the operating system before loading it
- Chain of trust operating system which authenticates application software before loading it
- Hardware secure boot process and Locking Critical Sections of Memory
- Protected memory (NVM/RAM/Cache) to avoid snooping and reverse engineering
- Encryption and anonymity
- Random Number Generation (RNG)
- Tamper detection
- Environment monitoring and internal control
- Trusted Execution Environment. Secure Code fetching & Execution (Integrity checks)
- Code and data signatures, built during compilation and stored and verified during execution
- A trusted storage of device identity and authentication means, including protection of keys at rest and in use
- Protection against unprivileged accessing security sensitive code.

Protection against local and physical attacks can be covered via functional security.

GP-TM-05: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow unauthenticated software, such software should only be run with limited permissions and/or sandbox.

GP-TM-16: Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.

GP-TM-28: Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them, and device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code. In order to minimise the potential for compromised code to access those code and/or data.

GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.

## 8. *Ensure that personal data is protected*

### *Stated UK Requirement*

Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this shall be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.

This guideline ensures that:

- i. IoT manufacturers, service providers and application developers adhere to data protection obligations when developing and delivering products and services;
- ii. Personal data is processed in accordance with data protection law;
- iii. Users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified;



iv. Users are provided with means to preserve their privacy by configuring device and service functionality appropriately.

*EU Requirement Mapping:*

GP-TM-10: Personal data must be collected and processed fairly and lawfully. The fairness principle specifically requires that personal data should never be collected and processed without the data subject's consent.

GP-TM-13: IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR). The complex mesh of stakeholders involved asks for/implies the necessity of a precise allocation of legal responsibilities among them with regard to the processing of the individual's personal data, based on the specificities of their respective interventions.

GP-OP-12: Data processed by a third-party (i.e., if the organisation utilises a cloud email provider), must be protected by a data processing agreement with the third-party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified.

GP-TM-11: Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed.

GP-OP-13: Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require that thirdparty service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorised access.

*Additional related elements:*

GP-PS-08: Privacy must be a guiding principle when designing and developing systems, in order to make privacy an integral part of the system.

GP-PS-09: Perform privacy impact assessments before any new applications are launched, using a top-down decomposition method that requires first answering three fundamental questions:

- Where is the targeted application deployed (Legal constraints and cultural significance)
- For what purpose (Scope)
- For which scenarios (Business requirements)

GP-TM-12: Minimise the data collected and retained. Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing).

GP-OP-09: Ensure the personnel practices promote privacy and security - train employees in good privacy and security practices for the secure usage of the systems, recognizing that technological expertise does not necessarily equate to security expertise.

GP-OP-10: Document and monitor the privacy and security training activities.

GP-TM-14: Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.

## 9. *Make systems resilient to outages*

### *Stated UK Requirement*

Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.

IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures may include building redundancy into services as well as mitigations against DDoS attacks. The level of resilience necessary should be proportionate and determined by usage but consideration should be given to others that may rely on the system, service or device as there may be a wider impact than expected.

### *EU Requirement Mapping:*

GP-TM-15: Design with system and operational disruption in mind. Build IoT devices to fail safely and securely, so that the failure does not lead to a greater systemic disruption. Have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water), preventing the system from causing unacceptable risk of injury or physical damage, protecting the environment against harm, and avoiding interruption of safety-critical processes.

GP-TM-17: Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems. A loss of communications shall not compromise the integrity of the device, and IoT devices should continue to function if the cloud back-end fails.

### *Additional related elements:*

GP-PS-03: Security must consider the risk to human safety.

GP-PS-04: Design for power conservation should not compromise security.

## 10. *Monitor system telemetry data*

### *Stated UK Requirement*

If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.

Monitoring telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimising security risk and allowing quick mitigation of problems. In accordance with Guideline eight, however, the processing of personal data should be kept to a minimum and consumers shall be provided with information on what data is collected and the reasons for this.

### *EU Requirement Mapping:*

GP-TM-51: Implement a DDoS-resistant and Load-Balancing infrastructure to protect the services against DDoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.

GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. The logs must also be preserved on durable storage and retrievable via an authenticated connection.

GP-OP-05: Establish procedures for analysing and handling security incidents. For any incident there should be a response to:

- a) confirm the nature and extent of the incident;
- b) take control of the situation;
- c) contain the incident; and
- d) communicate with stakeholders Establish management procedures in order to ensure a quick, effective and orderly response to information security incidents.

*Additional related elements:*

GP-PS-05: Design architecture by compartments to encapsulate elements in case of attacks.

GP-TM-31: Since some devices, gateways, etc. are required to be managed remotely rather than operated manually in the field, measures for tamper protection and detection are needed. Detection and reaction to hardware tampering should not rely on network connectivity. Hardware tampering means that an attacker has physical control of the device for some period of time. Broadly speaking, hardware tampering might occur at any of the different periods in the life cycle of a device.

GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed. There should be mechanisms to control device security settings, such as remotely locking or erasing contents of a device if the device has been stolen.

11. *Make it easy for consumers to delete personal data*

*Stated UK Requirement*

Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

IoT devices may change ownership and will eventually be recycled or disposed of. Mechanisms can be provided that allow the consumer to remain in control and remove personal data from services, devices and applications.

Requirement 11 is entirely a subset of an extended requirement eight.

12. *Make installation and maintenance of devices easy*

*Stated UK Requirement*

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.

Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats.

Requirement 12 is entirely a subset of extended features in other requirements.

13. *Validate input data*

*Stated UK Requirement*

Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

- i) Not of the expected type, for example executable code rather than user inputted text.
- ii) Out of range, for example a temperature value which is beyond the limits of a sensor.

*EU Requirement Mapping:*

GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering. Security is a concern for decision triggers (malware or general defects). Other possibilities here might be indirect manipulation of input values to the trigger by tampering with or restricting the input values. Reliability is a concern for decision triggers (general defects). Decision triggers could be inconsistent, self-contradictory, and incomplete. Understanding how bad data propagates to affect decision triggers is paramount. Failure to execute decision triggers at time may have undesired consequences.

GP-PS-01: Consider the security of the whole IoT system in a consistent and holistic approach along its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacturing, and deployment.

GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for trustable solutions and services. For example, a device measures its own integrity as part of boot, but does not validate those measurements - when the device applies to join a network, part of joining involves sending an integrity report for remote validation. If validation fails, the end point is diverted to a remediation network for action.

*Additional related elements:*

GP-PS-02: Ensure the ability to integrate different security policies and techniques, so as to ensure a consistent security control over the variety of devices and user networks in IoT.

GP-PS-07: For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.

GP-PS-11: Identify significant risks using a defence-in-depth approach. Conduct end-to-end risk assessments that account for both internal and third-party vendor risks, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded. Risk Assessment procedure should be initiated using a top-down decomposition method that requires first answering three fundamental questions:

- Where is the targeted application deployed (Legal constraints and cultural significance)
- For what purpose (Scope)
- For which scenarios (Business requirements)

GP-TM-21: Design the authentication and authorisation schemes (unique per device) based on the system-level threat models. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.

GP-TM-44: Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.

GP-TM-53: Avoid security issues when designing error messages. An error message should give/display only the concise information the user needs – it must not expose sensitive information that can be exploited by an attacker, such as an error ID, the version of the web server, etc.

UK Requirement	Covered EU Requirements	Related EU Requirements	Suggested Additions
No default passwords	GP-TM-09, GP-TM-22.	GP-TM-23.	GP-TM-25, GP-TM-26.
Implement a vulnerability disclosure policy	GP-OP-06, GP-OP-07, GP-OP-08.	-	GP-PS-06, GP-TM-57.
Keep software updated	GP-OP-01, GP-OP-02.	GP-TM-18, GP-OP-03.	GP-TM-19, GP-TM-20.
Securely store credentials and security-sensitive data	GP-TM-24, GP-TM-35, GP-TM-49.	-	GP-TM-40.
Communicate securely	GP-TM-34.	GP-TM-39.	GP-TM-36, GP-TM-37, GP-TM-38, GP-TM-41, GP-TM-52, GP-OP-04, GP-TM-07.
Minimise exposed attack surfaces	GP-TM-33, GP-TM-50.	GP-TM-45, GP-TM-43, GP-PS-12, GP-TM-08.	GP-TM-30.
Ensure software integrity	GP-TM-03, GP-TM-04, GP-TM-06.	-	GP-TM-01, GP-TM-02, GP-TM-05, GP-TM-16, GP-TM-28, GP-TM-56.

**Table 3 continued from previous page**

UK Requirement	Covered EU Requirements	Related EU Requirements	Suggested Additions
Ensure that personal data is protected	GP-TM-10, GP-TM-13, GP-OP-12.	GP-TM-11, GP-OP-13.	GP-PS-08, GP-PS-09, GP-TM-12, GP-OP-09, GP-OP-10, GP-TM-14.
Make systems resilient to outages	-	GP-TM-15, GP-TM-17.	GP-PS-03, GP-PS-04.
Monitor system telemetry data	-	GP-TM-51, GP-TM-55, GP-OP-05.	GP-PS-05, GP-TM-31, GP-TM-32.
Make it easy for consumers to delete personal data	Subset of Requirement Eight		
Make installation and maintenance of devices easy	Subset of extended features in other requirements		
Validate input data	GP-TM-54.	GP-PS-01, GP-TM-42.	GP-PS-02, GP-PS-07, GP-PS-11, GP-TM-21, GP-TM-44, GP-TM-53.

Table 3: Complete visual mapping of UK Requirements to EU Requirements

## 6 Suitability of Existing Proposal

### 6.1 Existing device classification

To determine how manufacturers may be pressured to improve security on their devices by this legislative effort, requirements specified as mandatory in the Secure by Design report have been applied to a selection of existing devices. Some flexibility has been given on the rules, as otherwise no meaningful data could be drawn. These are:

**Mandatory labelling.** No device will have the label already on their packaging before the label is defined. As such, no consideration will be made on the presence of this label.

**Vulnerability disclosure policy.** If a vulnerability disclosure program of any type already exists the product has been declared as meeting this requirement. This choice is justified as it would require only minor tweaking on the part of a company to comply.

**Software updates and end-of-life policy disclosure.** How long devices will receive software updates is supposed to be declared on the label, which does not exist. Therefore, if historical evidence exists of a product life-cycle with declarations being made of products meeting End of Life, and that products which are not declared End of Life receive updates, this requirement will be declared passed.

For the proposed scheme, no other requirements are considered when determining if a product passes or fails, so they have been ignored. It should additionally be noted that this mark scheme may be harsher than the current iteration of the Secure by Design requirements. As discussed in subsection 3.1, the current ETSI interpretation of the Secure by Design report has only 50% of the cumulative components of each of those first three requirements marked as mandatory. As such, if this is indeed what would be required, this marking scheme would need to be more lenient to more accurately effect existing device classification.

### **Method**

When determining if a device had the qualities tested for, many different locations were searched. These were the Terms of Service, any “Contact us” page (also checking a “Contact Us” on any parent company), site search functions, the hackerone directory, bugcrowd, and direct Google queries. Finally, links were explored around any reported vulnerabilities in the past, to see if they led to any information around future bug reporting.

The initial assessment was completed in 2019, and since then many web references have expired. Attempts were made to restore the original pages where possible, but this further heightens justification that the current system of manufacturers self-documenting may not be sustainable in the rapidly moving world of IoT devices. Limited revision of content has been performed where relevant (for example, if the device had been declared end of life, when there was no precedent for the company declaring end of life products) and any necessary large revisions have been noted.

### **Existing Devices**

#### 1. Amazon Dash Button

The device uses another device on the network for authentication, and has no default password [96]. The parent company has an existing vulnerability disclosure program [97]. The device has been declared end of life [98].

#### 2. Amazon Echo

Another mainstream IoT device, competing with the Google Home. Failures to meet requirements here after a competing product has passed certification could drive a change in policy to compete, justifying the government proposal. The device uses another device on the network for authentication, and has no default password [99]. The parent company has an existing vulnerability disclosure program [97]. The device has received software updates since launch [100] (the device is based on FireOS, a derivative of Android [101], and has been updated from being Android 5 based through to currently being Android 9 based). Other products have been declared end of life [98], however no existing Alexa/Echo products are yet old enough to have been declared End-Of-Life. As such, the Amazon Echo could be self-declared as meeting the requirements as set out by the UK government with no alterations (pending clarification on how they treat products which are declared end of life) and ship with the proposed Secure label.

### 3. Amazon Echo Spot

The device uses another service for authentication, and has no default password [102]. The parent company has an existing vulnerability disclosure program [97]. The device has received software updates since launch [100], while no existing Alexa/Echo products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.

4. August Doorbell Cam Note: All citations and information for this device broke between 2019 and 2022. The device uses another device on the network for authentication, and has no default password [103]. The parent company appears to have no existing vulnerability disclosure program (Company acquired by Assa Abloy who have a vulnerability disclosure policy in 2022) [104]. Although not explicitly stated, the Doorbell Cam appears to use the same mechanism for updates as the Smart Lock [105], while no existing products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.

5. August Smart Lock Note: All citations and information for this device broke between 2019 and 2022. The device uses another device on the network for authentication, and has no default password [106]. The parent company appears to have no existing vulnerability disclosure program (Company acquired by Assa Abloy who have a vulnerability disclosure policy in 2022) [104]. The device has received software updates since launch [105], while no existing products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.

### 6. BB8 SE Droid

The device links to a third-party device for authentication [107]. The parent company had an existing vulnerability disclosure program when first examined, which they have now closed down [108]. The device has received software updates [109], while no existing products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.

### 7. Belkin WeMo Insight Smart Plug

The device uses another device on the network for authentication, and has no default password [110]. The parent company has an existing vulnerability disclosure program [111]. The device can receive software updates and even notifies the consumer when these updates are ready to be installed [112], the parent company also explicitly declares when products are end-of-life [113]

### 8. Belkin WeMo MrCoffee Smart Coffeemaker

The device uses another device on the network for authentication, and has no default password [110]. The parent company has an existing vulnerability disclosure program [111]. The device can receive software updates and even notifies the consumer when these updates are ready to be installed [112], the parent company also explicitly declares when products are end-of-life [113]

### 9. Belkin WeMo Smart Light Switch

The device uses another device on the network for authentication, and has no default password [114] The parent company has an existing vulnerability disclosure program [111]. The device can receive software updates and even notifies the consumer when these updates are ready to be installed [112], the parent company also explicitly declares when products are end-of-life [113]



10. Bitdefender BOX IoT Security Solution The device has a default password from the factory, but it appears to be device unique [115]. The parent company has an existing vulnerability disclosure program [116] The device received software updates [117], and has been declared end-of-life [118].
11. Control4 EA-5 Controller  
The controller ships with a default “temporary” password [119] The parent company appears to have no existing vulnerability disclosure program. The device has received software updates [120], but relies on a third-party dealer to install them and to inform the customer if their products are End of Life [121].
12. Flow By Plume Labs Air Pollution Monitor  
The device uses another device on the network for authentication, and has no default password [122]. The parent company appears to have no existing vulnerability disclosure program. The device has received software updates and even notifies the consumer when these updates are ready to be installed [123], while no existing products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.
13. Foobot Air Quality Monitor Note: As of 2022 Airbox documentation is no longer accessible. Content has been migrated to Zendesk, which then removed this company. The device uses another device on the network for authentication, and has no default password [124]. The parent company appears to have no existing vulnerability disclosure program. The device has received software updates and even notifies the consumer when these updates are ready to be installed [125], while no existing products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.
14. Google Home  
The device uses another device on the network for authentication, and has no default password [126] The parent company has an existing vulnerability disclosure program [127] The device has received software updates since launch [128] and other Google products have an explicitly declared End-Of-Life date [129].
15. Linquet Bluetooth tracking sensors  
Linquet uses another device in Bluetooth range for authentication, and has no default password. [130]. The parent company appears to have no existing vulnerability disclosure program. The device has received software updates [130], while no existing products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.
16. Logitech Harmony Elite Universal Remote  
The device uses another device on the network for authentication, and has no default password [131]. The parent company has an existing vulnerability disclosure program [132] The device has received software update [133], and a device in the family has already been declared End-Of-Life with customers directly informed ahead of time [134].
17. Logitech Pop  
The device uses another device on the network for authentication, and has no default password [135]. The parent company has an existing vulnerability disclosure program [132]. The device has received software updates [136], the company has already declared products End-Of-Life and customers directly informed ahead of time [134]. Of note is that this product has been made End of Life, but customers were not informed, and it was not planned from device release.
18. Nest Cam Indoor camera  
The device uses another device on the network for authentication, and has no default password [137]. The parent company has an existing vulnerability disclosure program [127] The device has received software updates [138], other Google products have an explicitly declared End-Of-Life date [129].
19. Nest Cam Outdoor camera

The device uses another device on the network for authentication, and has no default password [137]. The parent company has an existing vulnerability disclosure program [127] The device has received software updates [138], other Google products have an explicitly declared End-Of-Life date [129].

#### 20. Nest Learning Thermostat

The device uses another device on the network for authentication, and has no default password [139]. The parent company has an existing vulnerability disclosure program [127] The device has received software updates [138], other Google products have an explicitly declared End-Of-Life date [129].

#### 21. Nest Smoke Alarm

The device uses another device on the network for authentication, and has no default password [140]. The parent company has an existing vulnerability disclosure program [127] The device has received software updates [138], other Google products have an explicitly declared End-Of-Life date [129].

#### 22. NETGEAR Orbi Ultra-Performance Mesh Wi-Fi

The device uses another device on the network for authentication, and has no default password [141]. The parent company has an existing vulnerability disclosure program [142] The device has received software updates [143], the company also explicitly declares when products are end of life to third party resellers [144]

#### 23. Particle Photon Wi-Fi with headers

The device uses a web account to login, phoning home on connection to the internet. [145]. The parent company appears to have no existing vulnerability disclosure program. The device has received software updates [146], the company also explicitly declares where products are in the lifecycle and when they are end of life [147].

#### 24. Phillips Hue Bulbs

The device uses another device on the network for authentication, and has no default password [148]. The devices have unique default identifiers from the manufacturers which are used for connection, but would still meet requirement. The parent company has an existing vulnerability disclosure program [149] The device has received software updates [150], and the product also has explicitly declared end-of-life products in the range [150]

#### 25. Phillips Hue Hue Go

The device uses another device on the network for authentication, and has no default password [151]. The parent company has an existing vulnerability disclosure program [149] The device has received software updates [150], and the product also has explicitly declared end-of-life products in the range [150].

#### 26. RING Doorbell

While not having a default password, authentication relies on IDs that cannot be changed. These, however, appear to be device unique [152]. The parent company has an existing vulnerability disclosure program [97]. The device has received software updates [153], while no existing products are yet old enough to have been declared End-Of-Life so no conclusions can be drawn.

#### 27. TrackR bravo Tracking Device

The device used another device on the network for authentication, and had no default password. The parent company appeared to have no existing vulnerability disclosure program. The device appeared to have no method for firmware update, and no products were declared End-Of-Life. The company instead vanished and shutdown all service, even their webdomain [154]

## 6.2 Interpretation

When interpreting the existing device classification, more devices passing should be regarded as a negative mark for the Secure by Design report's listed requirements. If too many devices are able to pass the requirements with no change to their functionality, it suggests that the requirements may not be sufficient to drive change in the Cyber Security of consumer IoT products.

To reiterate, a problem of significant scale has already been identified, and a voluntary approach was attempted [155, 51] ““The Government’s preference would be for the market to solve this problem - the clear security guidelines we set out will be expected by consumers and delivered by IoT producers. But if this does not happen, and quickly, then we will look to make these guidelines compulsory through law.””. Insufficient change was observed “change has not been swift enough, with poor security still commonplace.” [60] and it was decided that legal responsibility would be the only way to motivate the change required. As such, devices passing without having to make any changes is unlikely to bring any advancement to the field of IoT security.

As such, a new scheme certifying that few existing devices would have to change is cause for concern. However, the opposite is also true, that were many devices certified as failing these requirements it would be a sign that the Secure by Design report could effect significant changes in the industry, as was intended.

Figure 5 is a visualisation of the prior results.

As can be seen, only a single device outright fails the requirements (The Control4 EA-5 Controller, which is part of bespoke home automation systems). Five further received Minor Fails, which could be fixed in a matter of minutes, and a Sixth failed as the company dissolved without declaring products end-of-life. It seems apparent from this figure that the improvements to Cyber Security recommended in the Secure by Design report will be unable to effect change on the scale needed to tackle the issues identified in the IoT ecosystem.

Amazon Dash Button				Pass
Amazon Echo				Pass
Amazon Echo Spot				Pass
August Doorbell Cam				Pass (when revisited in 2022)
August Smart Lock				Pass (when revisited in 2022)
BB8 SE Droid				Closed vulnerability disclosure program
Belkin WeMo Insight Smart Plug				Pass
Belkin WeMo Mr Coffee Smart Coffeemaker				Pass
Belkin WeMo Smart Light Switch				Pass
Bitdefender BOX IoT Security Solution				Pass
Control4 EA-5 Controller				Fail
Flow By Plume Labs Air Pollution Monitor				Minor Fail, Vuln
Foobot Air Quality Monitor				Minor Fail, Vuln
Google Home				Pass
Linquet Bluetooth tracking sensors				Minor Fail, Vuln
Logitech Harmony Elite Universal Remote				Pass
Logitech Pop				Pass
Nest Cam Indoor camera				Pass
Nest Cam Outdoor camera				Pass
Nest Learning Thermostat				Pass
Nest Smoke Alarm				Pass
NETGEAR Orbi Ultra-Performance Mesh Wi-Fi				Pass
Particle Photon Wi-Fi with headers				Minor Fail, Vuln
Phillips Hue Bulbs				Pass
Phillips Hue Hue Go				Pass
RING Doorbell				Pass
TrackR bravo Tracking Device				Fail

Figure 5: Potential classification of existing IoT devices against UK Secure by Design Requirements, using the methodology specified in 6.1. The figure illustrates twenty-seven devices, each with three cells representing if they did or did not pass a requirement. In total, of those 81 cells, only seven are fails (three of which are in a single device), a home control smart device. Twenty devices pass completely with no changes required, and a further 5 could pass with adjustments to a Vulnerability Disclosure Program.

## Part III

# Improving UK IoT “Secure by Design” proposal through international standards

## 7 Improving the Requirements

### 7.1 European Requirement Mapping and Unmappable Requirements

To understand how best to improve these flawed UK requirements, the ENISA Baseline Security Requirements from subsection 5.2 have been taken as the foundation. This mapping allows them to be easily incorporated into a single reference document, and expresses the UK requirements in terms of related ENISA requirements, such that the ENISA requirements form a superset wholly encompassing the UK requirements.

Although the majority of the European Recommendations have a related category within the UK Recommendation, some are still out-of-scope. Were the UK requirements expanded to include every Related Requirement or Suggested Addition, a further three requirements would still be needed to wholly express the same domain covered by the ENISA Baseline Requirements European Recommendations (“IT Security Architecture”, “Identity/Access management” and “Security Governance & Risk Management”). These are as follows (numbering starts at 14, to continue on from the prior discussed requirements)

#### 14. *IT Security Architecture*

##### *EU Requirement Mapping:*

GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems.

GP-TM-48: Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set.

#### 15. *Identity and Access Management*

##### *EU Requirement Mapping:*

GP-TM-27: Limit the actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.

GP-TM-29: Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy.

#### 16. *Security Governance & Risk Management*

##### *EU Requirement Mapping:*

GP-TM-47: Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimise the overall risk.

GP-OP-11: Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs.

GP-OP-14: For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners.

As a visual aid, the following table now presents that additional information

Requirement	Covered EU Requirements
IT Security Architecture	GP-PS-10, GP-TM-48.
Identity and Access Management	GP-TM-27, GP-TM-29.
Security Governance & Risk Management	GP-TM-47, GP-OP-11, GP-OP-14.

Table 4: Mapping of extra EU Requirements into new 'UK-like' Requirements

## 7.2 Expanding Requirements

While incorporating these ENISA requirements has vastly improved coverage, some additional suggested improvements to be integrated have been identified (Marked with the text “Further Additions”, and a REQ code for identification) that further raise the potential ceiling for device security. The following comprises the superset of **all prior discussed requirements**, along with the full text of each subcomponent (where applicable). It can be considered the master/main of which all other discussed points are a subset.

'Includes' denotes the closest equivalent to the UK requirement, following “greater than or equal to”. Implementing 'Includes' will result in being at or beyond UK Requirement. 'Extend With' takes this further, with relatively minor changes or alterations that can provide significant improvement to the specification (intended as low hanging fruit). 'Additional Related Elements' begins to incorporate features that, while still related to the requirement, may have a degree of separation from the initial requested features. They may require significant development and incurred costs, or may be a change that otherwise involves work in areas that may not have been expected when interpreting the initial requirement. Lastly come 'Further Additions', which are the author's own suggested improvements. These are distinctly separated from the internationally recognised ENISA requirements, but are included as recommendations to address issues or gaps from the initial UK requirements which were not fixed by incorporating ENISA requirements alone.

### 1. No default passwords

#### *Stated UK Requirement*

All IoT device passwords must be unique and not resettable to any universal factory default value.

Many IoT devices are being sold with universal default usernames and passwords (such as 'admin, admin') which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed. Further details are available on the NCSC website.

<https://www.ncsc.gov.uk/collection/passwordshttps://pages.nist.gov/800-63-3/sp800-63b.html#sec5>

#### *Includes:*

GP-TM-09: Establish hard to crack device individual default passwords. Usernames and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked, and a hard to crack default password is still a weakness if it is used for more than one device.

GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.

*Extend with:*

GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates.

*Additional related elements:*

GP-TM-25: Protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts, or by making the user wait a certain amount of time to login again after a failed attempt. This protection should also consider keys stored in devices.

GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.

*Further Additions:*

REQ-1: Since IoT devices are advantaged over many other devices by having a near guaranteed internet connection, guidance around "weak" passwords can be enhanced with checks against a centrally stored database of common and frequently compromised password hashes. Over 40% of breaches identified in the Verizon DBIR report stemmed from credentials [156], and historically this number has been relatively consistent "Unauthorized access via default, shared, or stolen credentials constituted more than a third of the entire Hacking category and over half of all compromised records." This list of passwords is also something that can be updated easily, independently of individual devices, and force resets of passwords for new frequently appearing passwords. "Covid-2019" would have been regarded as a secure password up until 2018, but would now be exceedingly easy to guess.

## 2. Implement a vulnerability disclosure policy

*Stated UK Requirement*

All companies that provide internet-connected devices and services must provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

Knowing about a security vulnerability allows companies to respond. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Vulnerabilities should be reported directly to the affected stakeholders in the first instance. If that is not possible vulnerabilities may be reported to national authorities

<https://www.ncsc.gov.uk/contact>. Further details of the different approaches to take in different circumstances are included in the explanatory notes. Companies are also encouraged to share information with competent industry bodies <https://www.gsma.com/cvd>

*Includes:*

GP-OP-06: Coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT).

GP-OP-07: Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.

GP-OP-08: Create a publicly disclosed mechanism for vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.

*Additional related elements:*

GP-PS-06: For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.

GP-TM-57: The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches. Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.

*Further Additions:*

REQ-2: Include guarantees for the reporter of a vulnerability. Reports are treated confidentially or can be given anonymously, credit for vulnerabilities is offered and a guarantee of responding within ten working days is given (modelled after the GSMA's coordinated vulnerability disclosure policy) [82].

### 3. *Keep software updated*

*Stated UK Requirement*

Software components in internet-connected devices should be securely updatable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

The provenance of security patches should also be assured and they should be delivered over a secure channel. The basic functions of a device should continue to operate during an update wherever possible, for example a watch should continue to tell the time, a home thermostat should still operate and a lock should continue to unlock and lock. This may seem primarily a design consideration, but can become a critical safety issue for some types of devices and systems if not considered or managed correctly.

Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support shall be made clear to a consumer when purchasing the product. The retailer and/or manufacturers should inform the consumer that an update is required. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.

*Includes:*

GP-OP-01: Develop an end-of-life strategy for IoT products. Security patches and updates will eventually be discontinued for some IoT devices. Therefore, developers should prepare and communicate a product sunset plan from the initial stages to ensure that manufacturers and consumers are aware of the risks posed to a device beyond its expected expiry date.

GP-OP-02: Disclose the duration and end-of-life security and patch support (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase.



*Extend with:*

GP-TM-18: Ensure the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins. Failing to build in OTA update capabilities will leave devices exposed to threats and vulnerabilities for the entirety of their lifetimes.

GP-OP-03: Monitor the performance and patch known vulnerabilities up until the “end-of-support—” period of a product’s lifecycle. Due to the limited life cycle of many IoT devices, critical, publicly known security or privacy bugs will pose a risk to consumers using outdated devices.

*Additional related elements:*

GP-TM-19: Offer an automatic firmware update mechanism. Devices should be configured to check for the existence of firmware updates at frequent intervals. Automatic firmware updates should be enabled by default. A device may offer an option to disable automatic firmware updates and require authentication for it.

GP-TM-20: Backward compatibility of firmware updates. Automatic firmware updates should not change network protocol interfaces in any way that is incompatible with previous versions. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. Users should have the ability to approve, authorise or reject updates.

*Further Additions:*

REQ-3: Apply GP-TM-19 for software updates. Additionally, expand GP-TM-20’s “approve, authorise or reject” with more explicit offerings of “security updates only” and “no updates” as an option for device updates. Reverting updates, as with firmware, should be possible (even if it’s only to a factory state). Rejecting all updates and manually selecting specific updates should be entirely possible, to discourage abuse of updates to push anti-features and planned obsolescence. Devices should telegraph updates, especially if a reboot will be necessary. Automatic restart of device should be optional, and an estimated “down-time” for the device provided.

#### 4. *Securely store credentials and security-sensitive data*

*Stated UK Requirement*

Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.

Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys, device identifiers and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment and associated trusted, secure storage.

*Includes:*

GP-TM-24: Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.

GP-TM-35: Cryptographic keys must be securely managed. Encryption is only as robust as the ability for any encryption based system to keep the encryption key hidden. Cryptographic key management includes key generation, distribution, storage, and maintenance.

GP-TM-49: Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.

*Additional related elements:*

GP-TM-40: Ensure credentials are not exposed in internal or external network traffic.

*Further Additions:*

REQ-4: Expanding on GP-TM-24, credentials should be stored assuming the medium will eventually be compromised, effecting choice of encryption and token management. Discourage reliance on a third-party service for secure key storage. Every additional link in the chain is another attack surface which can be exploited. Instead, utilise strong first-party solutions from the project outset. Although integrated sub-processors for security management are currently regarded as a secure solution, their implementation should be taken under the advisement that they not only extend the attack surface, but (as of 2021) are being frequently observed to be subpar quality and relying on security through obscurity [157].

5. *Communicate securely*

*Stated UK Requirement*

Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.

The use of open, peer-reviewed internet standards is strongly encouraged.

*Includes:*

GP-TM-34: Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.

*Extend with:*

GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.

*Additional related elements:*

GP-TM-07: Use protocols and mechanisms able to represent and manage trust and trust relationships. Each communication channel must be trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions).

GP-TM-36: Build devices to be compatible with lightweight encryption and security techniques (including entities secure identification, secure configuration, etc.) that can, on the one hand, be usable on resource-constrained devices, and, on the other hand, be scalable so to minimise the management effort and maximise their usability.

GP-TM-37: Support scalable key management schemes. It has to be considered that tiny sensor nodes cannot provide all security features because they have lots of system limitations. Thus, the sensed data carried over infrastructure networks may not have strong encryption or security protection.

GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.

GP-TM-41: Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways). Data is often stored, cached, and processed by several nodes; not just sent from point A to point B. For these reasons, data should always be signed whenever and wherever the data is captured and stored.

GP-TM-52: Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.

GP-OP-04: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided. Purely proprietary approaches and standards limit interoperability and can severely hamper the potential of the Digital Single Market. Common open standards will help users access new innovative services, especially for SMEs, the public sector and the scientific community. In particular, the portability of applications and data between different providers is essential to avoid lock-in.

*Further Additions:*

REQ-5: Expand GP-TM-36 with specified “minimum compute hours to crack with current Year computers” for determining suitable encryption. This provides the advantage of increasing in difficulty automatically each year to correspond with advances in both cryptographic cracking techniques, new algorithmic vulnerabilities and rapid advances of technology (FPGAs/GPUs are now quite common, as well as many-core CPUs. Each of these rapidly advanced the computing power of computers, and subsequently their ability to crack encryption).

## 6. *Minimise exposed attack surfaces*

*Stated UK Requirement*

All devices and services should operate on the ‘principle of least privilege’; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

*Includes:*

GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.

GP-TM-50: Ensure only necessary ports are exposed and available.

*Extend with:*

GP-TM-08: Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default. Strong security controls should be something the consumer has to deliberately disable rather than deliberately enable.

GP-TM-43: IoT devices should be restrictive rather than permissive in communicating: When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.

GP-TM-45: Disable specific ports and/or network connections for selective connectivity. If necessary, provide users with guidelines to perform this process in the final implementation.

GP-PS-12: Identify the intended use and environment of a given IoT device. This will help developers and manufacturers determine the most suitable technical features for the IoT device’s operation, and the security measures required. This will also help to effectively handle bugs or enhancement requests.

*Additional related elements:*

GP-TM-30: Ensure a context-based security and privacy that reflects different levels of importance (e.g. emergency crisis, home automation).

*Further Additions:*

REQ-6: Include some pre-set behaviours tailored to expected use cases of the product. Customers using the same product for home as well as commercial applications will have different “correct” configurations. Prompts with different pre-sets could be easily implemented for most IoT devices, with potential network settings for “home”, “work”, “public”, or more advanced descriptions based on the relation of the device to other network infrastructure (connected directly to the internet, connected to another IoT device, connected to a router). Prompts for other configuration, such as data storage, (keep my data only on this device, allow my data to be communicated to other specified devices on the local network with an authorised key, allow my data to be accessible from the internet through an API) would help ensure that the device is properly configured for the use case the customer needs.

7. *Ensure software integrity*

*Stated UK Requirement*

Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

The ability to remotely recover from these situations should rely on a known good state, such as locally storing a known good version to enable safe recovery and updating of the device. This will avoid denial of service and costly recalls or maintenance visits, whilst managing the risk of potential takeover of the device by an attacker subverting update or other network communications mechanisms.

*Includes:*

GP-TM-03: The boot process initialises the main hardware components, and starts the operating system. Trust must be established in the boot environment before any trust in any other software or executable program can be claimed, so the booted environment must be verified and determined to be in an uncompromised state.

GP-TM-04: Sign code cryptographically to ensure it has not been tampered with after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded. Only run signed code and never unsigned code. Measuring the boot process enables the detection of manipulation of the host OS and software, so that malicious changes in the behaviour of the devices can be detected. It enables boot-time detection of rootkits, viruses and worms.

GP-TM-06: Restore Secure State - Enable a system to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful.

*Additional related elements:*

GP-TM-01: Employ a hardware-based immutable root of trust. The Hardware Root of Trust is a trusted hardware component which receives control at power-on. It then extends the chain of trust to other hardware, firmware, and software components. The Root of Trust should then be attestable by software agents running within and throughout the infrastructure.

GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, that provide:

- Chain of trust boot-loader which authenticates the operating system before loading it
- Chain of trust operating system which authenticates application software before loading it

- Hardware secure boot process and Locking Critical Sections of Memory
- Protected memory (NVM/RAM/Cache) to avoid snooping and reverse engineering
- Encryption and anonymity
- Random Number Generation (RNG)
- Tamper detection
- Environment monitoring and internal control
- Trusted Execution Environment. Secure Code fetching & Execution (Integrity checks)
- Code and data signatures, built during compilation and stored and verified during execution
- A trusted storage of device identity and authentication means, including protection of keys at rest and in use
- Protection against unprivileged accessing security sensitive code.

Protection against local and physical attacks can be covered via functional security.

GP-TM-05: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow unauthenticated software, such software should only be run with limited permissions and/or sandbox.

GP-TM-16: Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.

GP-TM-28: Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them, and device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code. in order to minimise the potential for compromised code to access those code and/or data.

GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.

*Further Additions:*

REQ-7: The suggestion of making Secure Boot mandatory would likely face challenge from consumer advocacy groups, especially with the manufacturer retaining the ability to reset their devices remotely. Such friction could be easily avoided by consulting with such groups ahead of time for this requirement, and have products labelled accordingly (Product is free to use and modify, product can be remotely reset by manufacture etc) such that products are lined up with the groups that expect those combinations.

8. *Ensure that personal data is protected*

*Stated UK Requirement*

Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this shall be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.

This guideline ensures that:

- i. IoT manufacturers, service providers and application developers adhere to data protection obligations when developing and delivering products and services;
- ii. Personal data is processed in accordance with data protection law;
- iii. Users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified;
- iv. Users are provided with means to preserve their privacy by configuring device and service functionality appropriately.

*Includes:*

GP-TM-10: Personal data must be collected and processed fairly and lawfully. The fairness principle specifically requires that personal data should never be collected and processed without the data subject's consent.

GP-TM-13: IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR). The complex mesh of stakeholders involved asks for/implies the necessity of a precise allocation of legal responsibilities among them with regard to the processing of the individual's personal data, based on the specificities of their respective interventions.

GP-OP-12: Data processed by a third-party (i.e., if the organisation utilises a cloud email provider), must be protected by a data processing agreement with the third-party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified.

*Extend with:*

GP-TM-11: Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed.

GP-OP-13: Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require that thirdparty service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorised access.

*Additional related elements:*

GP-PS-08: Privacy must be a guiding principle when designing and developing systems, in order to make privacy an integral part of the system. GP-PS-09: Perform privacy impact assessments before any new applications are launched, using a top-down decomposition method that requires first answering three fundamental questions:

- Where is the targeted application deployed (Legal constraints and cultural significance)
- For what purpose (Scope)
- For which scenarios (Business requirements)

GP-TM-12: Minimise the data collected and retained. Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing).

GP-OP-09: Ensure the personnel practices promote privacy and security - train employees in good privacy and security practices for the secure usage of the systems, recognizing that technological expertise does not necessarily equate to security expertise.

GP-OP-10: Document and monitor the privacy and security training activities.

GP-TM-14: Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.

*Further Additions:*

REQ-8: Although a factory reset is perceived as a way of securely removing personal data, this is not the case. Recovery of data on Android devices, for example, is not only possible but trivial. [95]. This shortcoming is especially notable as mobile devices will have similar power constraints to IoT devices. As such, factory resets should first encrypt the device volume before wiping it. This drastically reduces the risk of leaking sensitive data, as any information which can be recovered will be useless without the decryption key. Caution should still be advised however, as mobile devices in particular tend to use short decryption keys for ease of input, which opens them to brute force attacks [95]. Given the interfaces for IoT devices tend to be similarly compact, it is not unreasonable to expect that similar decisions regarding password length could be made. As the volume is not intended to ever be decrypted, a randomly generated key (that would be infeasible to use on such an interface-limited device) should be used to ensure data cannot be recovered via brute-force.

9. *Make systems resilient to outages*

*Stated UK Requirement*

Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.

IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures may include building redundancy into services as well as mitigations against DDoS attacks. The level of resilience necessary should be proportionate and determined by usage but consideration should be given to others that may rely on the system, service or device as there may be a wider impact than expected.

*Extend with:*

GP-TM-15: Design with system and operational disruption in mind. Build IoT devices to fail safely and securely, so that the failure does not lead to a greater systemic disruption. Have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water), preventing the system from causing unacceptable risk of injury or physical damage, protecting the environment against harm, and avoiding interruption of safety-critical processes.

GP-TM-17: Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems. A loss of communications shall not compromise the integrity of the device, and IoT devices should continue to function if the cloud back-end fails.

*Additional related elements:*

GP-PS-03: Security must consider the risk to human safety.

GP-PS-04: Design for power conservation should not compromise security.

*Further Additions:*

None

## 10. Monitor system telemetry data

### *Stated UK Requirement*

If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.

Monitoring telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimising security risk and allowing quick mitigation of problems. In accordance with Guideline eight, however, the processing of personal data should be kept to a minimum and consumers shall be provided with information on what data is collected and the reasons for this.

### *Extend with:*

GP-TM-51: Implement a DDoS-resistant and Load-Balancing infrastructure to protect the services against DDoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.

GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. The logs must also be preserved on durable storage and retrievable via an authenticated connection.

GP-OP-05: Establish procedures for analysing and handling security incidents. For any incident there should be a response to:

- a) confirm the nature and extent of the incident;
  - b) take control of the situation;
  - c) contain the incident; and
  - d) communicate with stakeholders
- Establish management procedures in order to ensure a quick, effective and orderly response to information security incidents.

### *Additional related elements:*

GP-PS-05: Design architecture by compartments to encapsulate elements in case of attacks.

GP-TM-31: Since some devices, gateways, etc. are required to be managed remotely rather than operated manually in the field, measures for tamper protection and detection are needed. Detection and reaction to hardware tampering should not rely on network connectivity. Hardware tampering means that an attacker has physical control of the device for some period of time. Broadly speaking, hardware tampering might occur at any of the different periods in the life cycle of a device.

GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed. There should be mechanisms to control device security settings, such as remotely locking or erasing contents of a device if the device has been stolen.

### *Further Additions:*

None. Although concerns were raised in the UK requirements, EU Recommendations alone address those concerns.

## 11. Make it easy for consumers to delete personal data

### *Stated UK Requirement*

Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

IoT devices may change ownership and will eventually be recycled or disposed of. Mechanisms can be provided that allow the consumer to remain in control and remove personal data from services, devices and applications.



This requirement is entirely a subset of the new requirement eight.

## 12. *Make installation and maintenance of devices easy*

### *Stated UK Requirement*

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.

Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats.

This requirement has been dissolved into logical extensions of other requirements.

## 13. *Validate input data*

### *Stated UK Requirement*

Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

- i) Not of the expected type, for example executable code rather than user inputted text.
- ii) Out of range, for example a temperature value which is beyond the limits of a sensor.

### *Includes:*

GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering. Security is a concern for decision triggers (malware or general defects). Other possibilities here might be indirect manipulation of input values to the trigger by tampering with or restricting the input values. Reliability is a concern for decision triggers (general defects). Decision triggers could be inconsistent, self-contradictory, and incomplete. Understanding how bad data propagates to affect decision triggers is paramount. Failure to execute decision triggers at time may have undesired consequences.

### *Extend with:*

GP-PS-01: Consider the security of the whole IoT system in a consistent and holistic approach along its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacturing, and deployment.

GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for trustable solutions and services. For example, a device measures its own integrity as part of boot, but does not validate those measurements - when the device applies to join a network, part of joining involves sending an integrity report for remote validation. If validation fails, the end point is diverted to a remediation network for action.

### *Additional related elements:*

GP-PS-02: Ensure the ability to integrate different security policies and techniques, so as to ensure a consistent security control over the variety of devices and user networks in IoT.

GP-PS-07: For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.

GP-PS-11: Identify significant risks using a defence-in-depth approach. Conduct end-to-end risk assessments that account for both internal and third-party vendor risks, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded. Risk Assessment procedure should be initiated using a top-down decomposition method that requires first answering three fundamental questions:

- Where is the targeted application deployed (Legal constraints and cultural significance)
- For what purpose (Scope)
- For which scenarios (Business requirements)

GP-TM-21: Design the authentication and authorisation schemes (unique per device) based on the system-level threat models. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.

GP-TM-44: Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.

GP-TM-53: Avoid security issues when designing error messages. An error message should give/display only the concise information the user needs – it must not expose sensitive information that can be exploited by an attacker, such as an error ID, the version of the web server, etc.

*Further Additions:*

None.

#### 14. *IT Security Architecture*

*Includes:*

GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems, to identify and authenticate of the assets involved in the IoT Service (i.e. Gateways, Endpoint devices, home network, roaming networks, service platforms, etc.).

GP-TM-48: Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set, since smart objects are often deployed as sets of identical or almost identical devices.

#### 15. *Identity and Access Management*

*Includes:*

GP-TM-27: Limit permissions of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users). Implement fine-grained authorisation mechanisms - such as Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC)- for executing privileged actions, access to files and directories, applications, etc. Use the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.

GP-TM-29: Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy. The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).

## 16. *Security Governance & Risk Management*

*Includes:*

GP-TM-47: Risk Segmentation - Splitting network elements into separate components to help isolate security breaches and minimise overall risk. Networks can be divided into isolated subnetworks to boost performance and improve security.

GP-OP-11: Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs.

GP-OP-14: For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners.

### ***Finalisation***

As expected from a superset of all requirements, there has been some identified overlap. These can now be removed to create a functionally equivalent set of requirements that now form the final recommended list. Each requirement is traceable back to its source, and the justification for any missing requirements (those that were identified as not needed) is documented above.

### ***7.3 Finished Categories***

The final recommendation is the following fourteen requirements. The source UK requirement (Or category created in the same manner as the UK requirements) is displayed in the first column. The remainder of the table details the source ENISA requirement, as well as a code for any personal recommendations (REQ-X).

UK Requirement	Covered EU Requirements	Related EU Requirements	Suggested Additions
1) No default passwords	GP-TM-09, GP-TM-22.	GP-TM-23.	GP-TM-25, GP-TM-26, REQ-1.
2) Implement a vulnerability disclosure policy	GP-OP-06, GP-OP-07, GP-OP-08.	-	GP-PS-06, GP-TM-57, REQ-2.
3) Keep software updated	GP-OP-01, GP-OP-02.	GP-TM-18, GP-OP-03.	GP-TM-19, GP-TM-20, REQ-3.
4) Securely store credentials and security-sensitive data	GP-TM-24, GP-TM-35, GP-TM-49.	-	GP-TM-40, REQ-4.
5) Communicate securely	GP-TM-34.	GP-TM-39.	GP-TM-36, GP-TM-37, GP-TM-38, GP-TM-41, GP-TM-52, GP-OP-04, GP-TM-07, REQ-5.
6) Minimise exposed attack surfaces	GP-TM-33, GP-TM-50.	GP-TM-45, GP-TM-43, GP-PS-12, GP-TM-08.	GP-TM-30, REQ-6.

**Table 5 continued from previous page**

UK Requirement	Covered EU Requirements	Related EU Requirements	Suggested Additions
7) Ensure software integrity	GP-TM-03, GP-TM-04, GP-TM-06.	-	GP-TM-01, GP-TM-02, GP-TM-05, GP-TM-16, GP-TM-28, GP-TM-56, REQ-7.
8) Ensure that personal data is protected	GP-TM-10, GP-TM-13, GP-OP-12.	GP-TM-11, GP-OP-13.	GP-PS-08, GP-PS-09, GP-TM-12, GP-OP-09, GP-OP-10, GP-TM-14, REQ-8.
9) Make systems resilient to outages	-	GP-TM-15, GP-TM-17.	GP-PS-03, GP-PS-04.
10) Monitor system telemetry data	-	GP-TM-51, GP-TM-55, GP-OP-05.	GP-PS-05, GP-TM-31, GP-TM-32.
11) Validate input data	GP-TM-54.	GP-PS-01, GP-TM-42.	GP-PS-02, GP-PS-07, GP-PS-11, GP-TM-21, GP-TM-44, GP-TM-53.
12) IT Security Architecture	GP-PS-10, GP-TM-48.	-	-
13) Identity and Access Management	GP-TM-27, GP-TM-29.	-	-


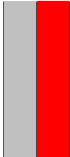
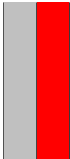



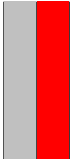
**Table 5 continued from previous page**

UK Requirement	Covered EU Requirements	Related EU Requirements	Suggested Additions
14) Security Governance & Risk Management	GP-TM-47, GP-OP-11, GP-OP-14.	-	-

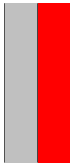
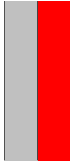




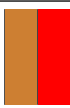





# 8 Existing device reclassification

If the author’s recommendations were integrated into the government proposal (pending confirmation of a pairing mode on pass devices) the following may be expected from device classification. For visualisation purposes, Bronze here indicates the device has met “Includes” requirements, Silver for “Extend with”, and Gold for “Additional related elements”. This decision is not a statement of support for that particular configuration, just a visualisation assistant. Note: A lot of the devices rely on Google, Amazon or Apple infrastructure. For both, the user email address is tied to a “user”. The discussion around whether this allows enumeration of users, and what extent this is an issue, could be the subject of a paper all on it’s own. As such, to keep focus on the intended target of this analysis, if a device ties to an Alphabet/Amazon/Apple account the various account related tests are carried over only in limited capacity. For example, “Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account” counts as a pass as there is no avenue for device enumeration without first compromising the entire associated account. The focus has shifted from attacking a device and it’s account, to now attacking an account and the device being the side-target. Owning the device has provided no additional vulnerability than what existed prior. Additionally, there is no realistic way to determine internal policy (for example, the existence of a CSIRT), so Requirement Two will check for the previously determined existence of a vulnerability disclosure policy, as well as trying to determine if a public record of past incidents is available.

In this simplified scenario with fewer requirements, the lowest result indicates rating (more advanced systems are proposed when considering labels and communicating with users, which can convey more detailed information). The third requirement is excluded, despite appearing previously, as the information required is not public. While this is an issue, it seems disingenuous to fail every device without exceedingly good reason.

IoT devices against expanded proposal		
Amazon Dash Button		Device deactivated by Amazon in 2019 [98]. Bluetooth/Wi-Fi pairing with no password.
Amazon Echo		Amazon Account to manage the paired devices. Not a Gold as Amazon Accounts can be enumerated, and Amazon do not consider this a vulnerability [158, 159, 97] Bug Bounty programs for AWS include all required criteria, but importantly this does not extend to other areas of Amazon, including their IoT devices. [97]
Amazon Echo Spot		Amazon Account to manage the paired devices. Not a Gold as Amazon Accounts can be enumerated, and Amazon do not consider this a vulnerability [158, 159, 97] Bug Bounty programs for AWS include all required criteria, but importantly this does not extend to other areas of Amazon, including their IoT devices. [97]
August Doorbell Cam		Updated website broke links. No silver [160]
August Smart Lock		Updated website broke links. No silver [160]
BB8 SE Droid		Bluetooth pairing with no password [107].
Belkin WeMo Insight Smart Plug		WeMo Account to manage the paired devices. Good [161], but not enough details to be sure of gold. Clarification of Account Management required. Although the Belkin Coordinated Vulnerability Disclosure Program is generous regarding post-patch disclosure, there is no indication they participate in information sharing to other stakeholders

**Table 6 continued from previous page**

IoT devices against expanded proposal		
Belkin WeMo Mr Coffee Smart Coffeemaker		WeMo Account to manage the paired devices. Good [161], but not enough details to be sure of gold. Clarification of Account Management required. Although the Belkin Coordinated Vulnerability Disclosure Program is generous regarding post-patch disclosure, there is no indication they participate in information sharing to other stakeholders
Belkin WeMo Smart Light Switch		WeMo Account to manage the paired devices. Good [161], but not enough details to be sure of gold. Clarification of Account Management required. Although the Belkin Coordinated Vulnerability Disclosure Program is generous regarding post-patch disclosure, there is no indication they participate in information sharing to other stakeholders
Bitdefender BOX IoT Security Solution		Additional layers harmed security by introducing a default password and not forcing it to be changed. It is a breach of the bitdefender bug bounty program terms to share with third parties at any stage, even post-patch, that the vulnerability existed.
Control4 EA-5 Controller		
Flow By Plume Labs Air Pollution Monitor		Web account to manage the paired devices [122]. Clarification of Account Management required.
Foobot Air Quality Monitor		1st Silver pending confirmation that pairing is locked behind an Account Login. Clarification of Account Management required.
Google Home		Google Account to manage the paired devices, but pairing involves no protections. Vulnerabilities disclosed through third-parties do not qualify for the protection of the vulnerability disclosure program.
Linquet Bluetooth tracking sensors		Device deactivated without notice in 2021. 1st Silver pending confirmation that pairing is locked behind an Account Login. Clarification of Account Management required.
Logitech Harmony Elite Universal Remote		Bluetooth/Wi-Fi pairing through an app, but documentation does not indicate an account and password are required. Silver were that clarified positively. Clarification of Account Management required. Logitech maintain internal and third party methods for vulnerability collection and provide few restrictions, even extending legal aid to participants if other third-parties attempt to prosecute against a responsible disclosure involving the bug bounty program.
Logitech Pop		Bluetooth/Wi-Fi pairing through an app, but documentation does not indicate an account and password are required. Silver were that clarified positively. Clarification of Account Management required. Logitech maintain internal and third party methods for vulnerability collection and provide few restrictions, even extending legal aid to participants if other third-parties attempt to prosecute against a responsible disclosure involving the bug bounty program.
Nest Cam Indoor camera		Device unique password used via QR code.
Nest Cam Outdoor camera		Device unique password used via QR code.



**Table 6 continued from previous page**

IoT devices against expanded proposal		
Nest Learning Thermostat		Nest Account to manage the paired devices [162]. Alphabet consider Enumeration not a vulnerability, will additionally actively assist in Enumeration [163].
Nest Smoke Alarm		Nest Account to manage the paired devices [162]. Alphabet consider Enumeration not a vulnerability, will additionally actively assist in Enumeration [163].
NETGEAR Orbi Ultra-Performance Mesh Wi-Fi		Netgear Account to manage the paired devices. Clarification of Account Management required. It is a breach of the vulnerability reporting terms and conditions to discuss a vulnerability without explicit permission, even after the issue is resolved [164]
Particle Photon Wi-Fi with headers		Email and Account are tied, with the devices tied to the email address. Concerning security implications for OTA updates.
Phillips Hue Bulbs		Pairing through app with no password. Pairing uses an unchangeable device unique identifier (MAC address). The bulbs also have other unique unchangeable identifiers. Phillips will publicly declare an issue once patched if the researcher requests this. Additionally state that lessons learned are shared directly back to development teams, with the vulnerability and it's information being non-proprietary and non-confidential.
Phillips Hue Hue Go		Pairing through app with no password.
RING Doorbell		Ring Account to manage the paired devices. Not a Gold as Amazon Accounts can be enumerated, and Amazon do not consider this a vulnerability [158, 159, 97]
TrackR bravo Tracking Device		Unable to verify any functionality beyond 1st Bronze.

Table 6: IoT devices against expanded proposal

This simplistic representation helps show the potential gains that may come from implementing a certification scheme with a much higher ceiling. Not only do we have stratification of devices which were previously only represented as equals, but also the ability to make informed choices. If priorities lie in Responsible Disclosure, the information is available to know the limitations of otherwise reputable Amazon and Google devices. With just two columns, the available expression of data per device is now sixteen bits of information (previously four bits) and this has had clear impact on usability of the standard. This is without the additional information coming from not only the comments but also by comparing information between many competing devices. These benefits from growing available data will be remembered as the next phases of the project continue.

## Part IV

# Developing a usable IoT Cyber Security label for point-of-sale solutions

## 9 Existing Label Proposal

### 9.1 *Why is a label the preferred catalyst for security improvement in IoT devices?*

A new trend which is emerging in the consumer marketplace is for, rather than a singular high-power device being the focus of all internet connected activities, instead to have networks of low power devices which are connected directly to the internet. These Internet of Things devices (IoT) have surged in popularity, with new products being rushed to market to cash in on the trend. However, in the rush to market, many manufacturers are overlooking even basic security and privacy protections for their devices. As such, many consumers (both personal and business) are inadvertently opening themselves to cyber attacks by incorporating these devices into their environment, which are costly to the UK (and global) economy. A proposed solution by the UK government is a label on products which denotes whether they have met a minimum security standard, with this action supported by two reports. The first, by “Harris Interactive”, contains several different label designs proposed by the DCMS, while the other report was conducted by the DCMS itself, and is a study of existing product labelling systems.

The Harris Interactive report [58] is concerned with gathering evidence regarding the general public with relation to IoT security, to ensure the public is “fully informed about the safety and security features of IoT (Internet of Things) devices”. Within this report, several important statistics can be observed which are of particular importance when justifying the creation of a standardised security label. Of particular note was that, of those customers who did not rank security features in their top four considerations when buying a device, this was frequently declared to be because consumers largely assume that security is already built-in. In fact, 72% of all respondents believed security features were already in-place when the products arrived on the market. 73% of those questioned felt a security label is an important addition to products, with 44% of those describing it as very important. Additionally, the Harris Interactive report indicated that consumers are willing to pay a small premium for a security labelled product (under ten percent of a product’s price), the amount varying for the type of device.

The other DCMS commissioned report [165] highlights the current state of labelling in the marketplace, and how manufacturers frequently display their certifications with prominence. This is justification for manufacturer’s finding value in a label and certification program for their products. Particularly highlighted in the report was a specific instance of a label on a Toshiba Smart TV, featuring certification from the Bavarian Government, that was displayed prominently on the product’s page.

“One particularly relevant label found was on the Toshiba - 24W3863DB 24-Inch HD Ready Smart TV with Freeview Play manufacturer website. A whole section of the product features page is dedicated to ‘Secure Smart TV: Proving how seriously we take your right to privacy, we have become the first TV brand to be certified and approved as secure by the Bavarian State Government.’ Although only found in one instance, the prominence placed on this certification by the manufacturer shows it is valued highly as part of their communications and marketing of the product.”

Together, these two reports provide a strong mandate for adopting a label for the purpose of communicating a standard of cybersecurity to a consumer at the point-of-sale. Through this, it can be expected that consumers will better understand what devices may or may not be suitable to integrate into their networks, informing their purchasing decisions and feeding back to increase the number of devices which incorporate a higher standard of security.

## **9.2 Process to acquire Harris Interactive proposed label**

The current proposal for acquiring a label is as follows: “Option A (preferred option): Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self declare and implement a security label on their consumer IoT products. The Government is developing a product security labelling scheme which will first be voluntary and then mandated once the relevant bill has achieved royal assent. The voluntary labelling scheme will contain the same requirement as set out in this proposed option. The label must indicate whether the product adheres to the following three aspects of the Code of Practice, namely that:

- All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.
- The manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues.
- Manufacturers will explicitly state the minimum length of time for which the product will receive security updates

”

Of the several proposals the government has outlined, this is their preferred option and the most likely to become law. There were five different choices outlined, briefly summarised these were :

“

- Option One: Do nothing (i.e. no regulation). Manufacturers can choose whether to implement the UK Government’s voluntary label or voluntarily pledge to implement the Code of Practice guidelines.
- Option Two: Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self assess and implement a security label on their consumer IoT products. (Preferred option)
- Option Three: Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with manufacturers to self assess that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security.
- Option Four: Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers to self assess and to ensure that the label is on the appropriate product packaging.
- Option Five: Adopt a potential consumer IoT certification scheme that may emerge from the EU cyber security certification framework being established by the EU Cybersecurity Act

”

Of these options, the government has justified that action must be taken due to the lack of uptake for these requirements by industry since it first announced them as voluntary in October of 2018, eliminating option One. It has further justified that a label is required due to the current difficulty for consumers to distinguish between devices with high and low quality security features, eliminating option three. Justification is not provided for discounting Option Five, it is mentioned as a possibility to be negotiated during a possible withdrawal agreement with the European Union but not considered further as an alternative to the other proposals. Remaining are options Two and Four, which are to label whether or not a product meets three requirements or to mandate meeting every requirement and additionally label that they do so. This researcher finds it unusual that there was not more granularity to this choice, as usually it would be expected to have more options than requiring a product meet 0% and 100% of requirements to be sold on the UK market. Additionally, the option of mandating that a specified three requirements be mandatory was unnecessarily eliminated by not including the label in the description of this option. Of the two remaining options, Option Four was determined to be stifling to innovation and neither practical or cost effective. As such, by process of elimination, option Two remains the sole option for the government to proceed with.

Option Two requires only that a manufacturer self-certify that they do or do not meet the base three requirements, labelling their product as such. No regulatory power exists to mandate that products do meet these requirements, or to prosecute any manufacturer who does not meet these basic security requirements. Given that the manufacturers self-certify, it is presumed that manufacturers who falsify or otherwise are dishonest about their product when submitting certification will be prosecuted under other existing laws.

Under this proposed process, manufacturers will have to decide ahead of time whether or not they wish their product to be certified as meeting the security requirements set out by the government's proposal. If they do wish to meet the requirements, and during their self-certification process they determine they in fact meet the requirements, they may display so on their label. Otherwise, they have the choice to redesign the product such that it meets requirement or to proceed with the product not meeting requirement. Whether they failed to meet requirement, or decided never to attempt to do so, they must still display a security label showing that they do not meet the standards set out by the Government.

### **9.3 Discussion Points**

#### **9.3.1 Potential alternate processes involving Harris Interactive proposed label**

As briefly mentioned within "Process to acquire proposed label", the proposed recommendations are extremely coarse in nature, perhaps to create the illusion of choice while steering the conclusions of any investigation to a specific desired outcome. Whatever the reason for the discrepancies observed, this should be the first component to be addressed. If the recommendations which the Government's proposed recommendations are built on top of are flawed, it renders all other efforts moot. Ranked from "Most Helpful" to "Most Damaging" are a selection of potential courses of action, with the government's own proposals included. While based on practices from different related topics and historical precedent, these rankings are still opinion and should not be mistaken for fact.

- Case One: More granularity. The seemingly obvious and correct solution is to conduct additional testing with a wider range of configurations, determining the best outcome for all parties involved. When doubt is raised, the correct scientific response is to conduct more testing. Possibilities include varying the number of requirements to satisfy for a label, different designs for labels (bronze/silver/gold?) and re-run studies with these variables to determine the best option for consumers. Also re-evaluate the scope of the requirements chosen, many recommended changes would be cheap to implement for all parties in terms of both cost and time.

- Case Two: Alter the label (How many requirements are met). “Gold, Silver, Bronze, Fail”. If the requirements themselves cannot be altered, an alternate way of introducing additional granularity to this label is to have additional classifications than the binary pass/fail. Having a bronze be meeting three requirements and a gold for meeting 10 would drive competition between companies to improve their design process for the coveted gold standard. If the requirements do change or expand, A-E could fit nicely too, being familiar to consumers from Gas/Electricity efficiency ratings.
- Case Three: Alter the label (Add a year). If neither the requirements or the number of requirements that have to be met can be altered, add a “Year of Certification” to the label. This introduces the possibility of quickly adapting to the rapidly changing digital environment, with speeds that are not comparable to other fields, acknowledging the need for swift responses to new threats. The Government has already acknowledged how difficult it can be to effectively assess the field, with the original proposal being a purely voluntary scheme (modelled on the success of similar schemes in other fields). However, this had to be revised to the current mandatory proposal when it was realised that companies operating in the IoT market are not driven by the same factors as conventional distributors. Note: This proposal is still harmful to the security landscape when compared to the above recommendations, as there will be a years long tail of insecure devices after any change is made (if something were 2016 certified, customers are unlikely to view it as insecure and replace it in 2018). However, this case is still less harmful than the current proposal and a good step in the right direction.
- Case Four: Remove the label altogether. If the label cannot be altered in any way, no requirements can be altered and the number of requirements required for certification also cannot be changed, remove the label altogether. In the digital landscape, the illusion of security is extremely harmful to the health of the ecosystem. In other fields, “security theatre” can be conducted to reassure the public with no harm to the landscape as a whole, simply increasing sales. The inclusion of fake security does not harm actual security, as it still exists. However, creating the illusion of security where there is none in the digital landscape is what leads to some of the most damaging attacks, as devices are integrated into otherwise secure networks under the belief that they too are secure, compromising the entire system. As mentioned above, the Government has recognised this field may not be entirely what they expect when they had to revise their voluntary plan. This recommendation is, essentially, a request to acknowledge that this may still be the case and to allow the dust to settle before they decide what standard devices will have to meet before being plastered with a label saying “secure”.
- Case Five: Scrap all aspects of the proposal. If the Government refuses to modify this proposal in any way, and the label itself is part of the whole package, scrap and start the process again. As mentioned, it is extremely harmful to proceed with a false illusion of security. It would do the UK economy less harm overall to scrap the entire proposal and either wait for the ENISA requirements and decide whether to adopt them, or start the entire process again to determine new requirements.

Options below this point are actively detrimental to the long term health of Cybersecurity in the UK:

- Case Six: Make the existing three requirements mandatory, rather than optional. If the requirements can’t be altered, and the boundary for meeting requirements can’t be altered, make the existing minimum mandatory. This would be more harmful than any of the other proposed options, except keeping the current proposed plan, for the reasons outlined below.

- Case Seven: Use the current proposal as-is. Extraordinarily harmful to long term security, for short term gain. The proposal states a percent of cyberattacks that would be prevented by these changes (the default password, for example). However, this is conflated with the expectation of significantly reducing the total number of cyber attacks that would occur (shown in the cost/savings estimates, loss due to cyberattack is expected to drop massively). This reduction and cost savings are, however, unlikely to be accurate in practice. Such a large percentage of cyber attacks use “default passwords” as an avenue attack because it is the easiest method. Removing the option to target through “default passwords” attacks should be expected to stop those attackers from continuing, as they will simply target the next weakest point of entry. Were this new entry point to carry with it a significantly higher cost in terms of time or effort, the total number of successful attacks (and corresponding monetary value lost by victims) would be expected to drop significantly. This is not the case, however, as even a device which meets the government’s guidelines (which devices are not mandated to do) would still be vulnerable with a similarly low barrier to entry. When factoring in the expected continual growth of the IoT sector, the damages incurred may still increase with not just the quantity of IoT devices, but also through the introduction of devices covering additional surface area, giving potential to increased value from compromising targets. For example, IoT devices currently handle confidential and otherwise sensitive data rarely, yet are already valuable enough to target. As they become more ingrained in day-to-day life, more and more confidential and valuable data can be collected by these devices, increasing the value of compromising them. Recommendation Four is not included for certification, which is that devices must secure credentials securely. IoT payment helpers are already appearing, and the future likely includes only more and more valuable targets to compromise. As a thought experiment around a single IoT Device “Fridges that order you replacements online automatically when you use up the last of a product”, how many different valuable credentials could be gathered from compromising a singular device? (People per house authorised on the device) multiplied by (number of online websites that device can interface with (all possible, not just those already used, not all fridge items are on Amazon)) multiplied by (number of payment processors that the websites accept (Google Pay, PayPal, Visa. . .)). Elaborating that math, how many fraudulent Google Pay transactions could occur before lock out? Then an attacker could switch to using the next payment provider, PayPal, until it’s locked out. Then all they can for Visa. . . this process then repeats for every person registered on that device. Significant financial gain suddenly becomes viable from compromising single devices again.

### **9.3.2 Label**

The label itself is an amazing proposal, a brilliant way of communicating a complicated concept to an average consumer in a way that they can understand. Outlined in the Harris Interactive report, the proposed label is recognisable and effective at communicating the intended information to the consumer. The only caution would be that, while the label is recognisable and understandable in isolation, will it be as effective on a box when the product is surrounded by other labels with a similar colour scheme that consumers have been internally training themselves to ignore? Additional testing would have to be conducted to determine this, as well as what any potential remedies might be. The works undertaken are unfortunately undermined by a low bar to pass for certification, with little incentive for a manufacturer to strive for better. This comes at a time where other organisations (such as ENISA) are choosing to raise both the acceptable minimum, but also the potential ceiling for security in devices. As previously mentioned, the current plan also does not include provisions for future revisions, or any plans for the requested frequent reviews requested in the Harris Interactive report [58].

### **9.3.3 Why the current label is insufficient; Additional information to take into account when trying to determine the structure of a new label**

To determine the best possible structure of any new label, other proposals which each have their own successes and failures have been analysed. Customers making informed purchases at the point-of-sale is beneficial for altering consumer behaviour [166], and many success stories exist in the OECD good-practice examples of Energy products. Corresponding positive effects were additionally observed through this alteration of consumer behaviour, with long-term pressures emerging on manufacturers adjacent to even a voluntary label.

As Energy Usage is quite a simple metric to convey, a more complex parallel was sought in food labels. Nutritional Information panels on food have to convey a complicated subject with nuance and context, with the need for potential customers to still be able to quickly assess a product. ““Consumers require accurate, standardized and comprehensible information on the content of food items in order to make healthy choices. Governments may require information to be provided on key nutritional aspects, as proposed in the Codex Guidelines on Nutrition Labelling” “International standards. Public health efforts may be strengthened by the use of international norms and standards, particularly those drawn-up by the Codex Alimentarius Commission. Areas for further development could include: labelling to allow consumers to be better informed about the benefits and content of foods” [167]”

Here, front-of-pack labels (FoPLs) seem to have been quite successful for allowing customers to make more informed purchases at the point-of-sale, which seems to have additionally incentivised manufacturers to reformulate their products to achieve higher ratings for their FoPL [168].

Even if all information were available, it can be overwhelming for consumers to digest such information at the point of sale. A meaningful label parallels the solution proposed here, of signpost labelling. “The provision of detailed dietary information at the back of food packages (e.g., nutrition-fact panels in the form of a table or a grid) started to appear on food packages at about the same time period and was expected to have long-term positive effects on consumers’ food choices(Kozup et al., 2003). However, putting this general advice into practice appeared not to be straightforward for consumers.” “...need of more intuitive systems was felt. As a result, the focus in the last decade has moved toward more product-oriented and practical tools to help people make better choices. Nutrition signpost labelling is seen as an important and practical tool to assist consumers when making food choices” [169]

Regarding how this label should be presented, the evolution of the European Union energy label provides some insight into what may be effective for consumers as well as what challenges the label could face from successive years of implementation. Originally, the labels were A to G, with G being the least efficient. However, as technology advanced, what was once considered an A-class piece of equipment could be vastly less efficient than a newly released piece of technology. The chosen solution was to append successive + ratings onto the existing A category, giving A+ A++ and A+++ . Any labelling for IoT devices risks the same problem. As technology advances, what was once reasonable encryption can quickly become obsolete. As the power of general computers grows, the time to crack encryption decreases. Additionally, there is the potential for rapid movement in the IoT space. Whether advances in Cracking methodology/technology (such as occurred with GPU clusters) or if flaws are discovered in specific implementations, what was once highly secure encryption could suddenly become feasible to crack. The product itself does not have to be flawed for this to occur, and developments in the world of CyberSecurity are a situation with few parallels. No new discovery about Electricity will cause devices with European Union energy labels to suddenly lose massive efficiency, which would require them to jump down several categories.

Of note is that the EU energy labels are changing back to their original A-G method for ranking [170], as the revised method was deemed to not be differentiating between products enough, and had strayed too far from it’s goal of being simple.

Given a goal of this project is that the suggested recommendations (if implemented) provide significant benefit to user-space, a significant amount of time and effort should be devoted to appropriately assessing how best to deliver that goal. Initially, it was planned that this testing be integrated into the current project, however due to the emergence of Coronavirus this has been significantly scaled down. Based on similar works [171, 74], and the previously mentioned findings of the Harris Interactive report [58], enough information is present to begin prototyping consumer focused labelling in IoT devices.

#### **9.4 Key characteristics identified and label objectives**

From a detailed reading of the above discussed reports and their findings, it has become clear that for the label to succeed the iconography must be a key focus point of the design process.

Icons should avoid text to remain **language independent**, as the label is intended to be usable by all. This is a well established part of Human Computer Interaction [172], that where possible it is better to encourage recognition rather than recall.

The Iconography should also be **uniquely identifiable**, such that it cannot be confused with other pre-existing or future symbology. This is distinct from the idea of building on existing symbology and themes; Their themes can be incorporated, but the iconography should still be distinct.

Where possible, iconography should **convey meaning**, without any accompanying explanation. Explanation being necessary removes some of the primary benefits of iconography, such as being able to transcend language barriers. This is an exceedingly difficult task [173], and though it will be aimed for, conveying meaning via iconography is not expected to be successful in all aspects.

- If absolutely necessary, explanations should be short and easy to understand to even first time users.
- Technical “jargon” should be avoided, using user-friendly language.
- The explanation should be memorable, such that a user should remember what the iconography signifies and should (ideally) never again need to revisit the explanation.

Where possible, reusing pre-existing established metaphors from the security and wider landscape (for example, a Lock for Secure) should be prioritised to reduce any learning overhead. Additionally, attempting to incorporate iconography which users may already be familiar with from other efforts (for example, USB for “attack surface” links well with what many businesses teach in basic Cyber Security training).

The Energy Efficiency labels provide a cautionary tale around planning for future advances. As it is so difficult to predict the future of Cyber Security (new flaws could be discovered in an encryption algorithm any day, suddenly rendering a method inadequate), it is important to instead tie certification to some date in time. This allows recalibration each release of the label, to rapidly reclassify when needed.

Further recommendations from User Experiences specialists provide many further notable points, which were considered during the design process [174]. Although all important, some specific examples are on Relative Size of iconography and to be visually simple. While little could be applied from the broader principles of Human-Computer Interaction due to the demands for consistency of design in all GOV websites, materials were kept in mind during the design process in case opportunities presented themselves (of particular note, the works of Ben Shneiderman [175]).



## **10 Own Proposed Label**

### **10.1 Main Proposal**

Following the determination of the 14 requirements and the prior characteristics desired for a label, the following draft versions of a comprehensive proposal have been created. These collectively make the V1 proposal, with their variations indicated in the form V1.x. 196 bits of information are directly expressed via the binary expression of Tick or Cross.

#### ***A comment on iconography:***

Security requirements can be complex, with many intricacies. Although the overhead for each has been significantly reduced with simplified explanations, further reducing them to understanding in the space of an icon proved to be an exceedingly difficult task. As such, an alternate objective was provided when designing the iconography. To inspire curiosity. The worst fate for iconography that intends to inform the consumer would be to have it be completely ignored, with eyes that glaze over. As such, given that it was likely at least some consumers would require an explanation, the iconography was designed with the goal of encouraging users to look up that explanation out of curiosity at least once. To aid with this, the largest single feature on the label is (rather than any of the iconography) the three word code for looking up the additional information. As the most prominent feature, it is intended that this should make it clear to users that this feature is something that may be worth paying attention to and investigating. Combining this prominent feature for looking up additional information with the aforementioned explicit design goal of inspiring curiosity, the author hopes the combination will be effective for driving users towards the definitions whenever they cannot understand an icon.

## Features

The current working title is presented, “United Kingdom IoT Security Certification Scheme” as a sufficiently long title such that (were the proposal accepted) the official titling chosen by the DCMS would likely fit within the space of the label. A subtitle “Summary of Assessment” was chosen, as a descriptor that would function independent of any titling changes that may appear from adoption of the label. Building on the established iconography for Security, a Shield is used as part of the logo. The refresh icon is intended to show this as something continuous, not static, and the tick to show that this is a good icon to receive. The message as a whole then being that this label is a Security-Related label, with some continuous aspect and it’s presence here is positive. Immediately below this is “Version 2021 certified” (Or alternate information in variations) to explain the Continuous aspect of the icon, installing an expectation that there may be versions for other years too. From here, the main body of the label is divided logically into three columns and five rows (15 cells). The three columns are further subdivided in a 2/3 to 1/3 ratio, with 2/3rds of the column space devoted to the Requirement Icon, and 1/3rd to a Tick or Cross related to the requirement. Only the Horizontal grid-lines are visible, rather than no grid-lines, just the vertical grid-lines or both vertical and horizontal grid-lines, as during design informal feedback the other lines were described as crowded and the lack of any lines left people confused on which Requirements/tick-cross were paired. There was a conscious choice to ensure lots of whitespace was present, as other related works (such as food labelling) can especially become crowded. It is intended that, if the label were too large or there were too much whitespace, it is easier to gradually reduce it until an “acceptable” threshold is reached rather than try to guess where whitespace may be needed from feedback of “too cramped”. As there are only 14 requirements and 15 cells, the final cell is devoted to summing up the information conveyed. So that consumers do not have to count (and to make it even more clear that a cross means that this requirement didn’t pass) a total out of 14 requirement met statement is made. To ease consumer worry about seeing potentially many crosses on a device, there is also a “Pass” statement to let consumers know that this level of security is still legally “acceptable”. Lastly, the bottom fifth of the label is devoted to finding out more information. It contains not only context that this label is part of a Cyber Security scheme to determine if a product is fit for sale in the UK, but that this product has succeeded in that assessment. A statement that more information is available is included (with instructions) and the largest single element of the entire label is the eye-grabbing three-word-code that ties this device to it’s full assessment. This particular feature was chosen as different versions in the same line of IoT devices can be hard to distinguish from each other, especially before you can access the manual. Two near-identical looking devices in similar packaging will still have differentiation in their unique assessment codes. A three-word-code was chosen over a QR code due to the reasons outline in 4.1, specifically around accessibility for all age bands in the United Kingdom.

The first version (V1.1) is the simplest prototype, with a year plainly presented for when this device was certified. The prototype is effective at conveying the intent that the date of certification is important, however not why it may be important. With this naïve implementation, if a device were certified in 2022 and a competitor in 2023, there is no guarantee that the second device were any more secure than the first. As such, an immediate amendment to this proposal is for the Year field on devices to signify not the year they are certified, but the year of the legislation they are certified against. The current proposal is for this legislation to be reviewed every two years [59] which would make for a easy to understand system. However, were this commitment not upheld and significant periods of time to pass between legislation revisions, seeing certifications with a date many years ago could harm consumer confidence. This would also further amplify the negative of this label, that it is unclear why it matters which year a device displays.

The second variation (V1.2) is a version numbering system. Intended to iterate yearly, even if there were no change to requirements, a version number provides an easy way for consumers to look up what requirements were in force when the device was certified. As before, an immediate logical amendment is to tie the version numbers to iterations of the legislation that the label is certified against. A significant downside to version numbering is that they lack any implicit context; in a vacuum these numbers mean nothing. If there were a commitment to revise relevant legislation at least every two years, it is easy to see that within decades version numbering could become confusing. Without the presence of a current-generation device on the shelves to provide context, old devices can still display high version numbers, giving the illusion that they are secure and up-to-date. However, the version numbering system becomes more robust in scenarios where the pledge to revise legislation frequently is not kept. Were five years present between iterations, this is a sufficient period of time for a raised version number to become noticeable on store shelves.

## **10.2 Alternate Proposal**

While the case has been strongly made in this paper for a comprehensive solution for Cyber Security information at the point-of-sale, the reality is that the current proposal for a simple label has already undergone three years of public consultation and investment. Such a fundamental redesign would require re-engaging with Industry, fresh consultations and potentially set the process back to zero. Even if the comprehensive proposal faced no significant opposition from groups during consultation, it is not unreasonable to assume that a similar timescale would face the new proposal.

Currently, consumers have no point-of-sale information, and no market protections exist against insecure IoT devices. As such, adopting the advanced label could have the consequence of a further three-years (at the lower bound) with deployment of insecure infrastructure, during a period of exponential growth in the sector. However, as stated earlier in subsection 9.3.1, if the proposal were to just proceed with a poor label implementation it could undermine future efforts to secure UK IoT infrastructure. The following are variations on a simpler label, similar to that which has already been approved by stakeholders, whilst reducing the potential for long-term harm. This reduction in harm is accomplished primarily by adding some method of dating certification of the device into the displayed information, such that out-mode devices are easily identifiable. This series of labels, as part of the same “generation” proposal as the Main proposal, will be referred to as part of the V1m.x series (Version 1, mini, variation number) Variations on Year and Version number are present, for the same reasons as the V1 label.

### 10.3 Label 1.0

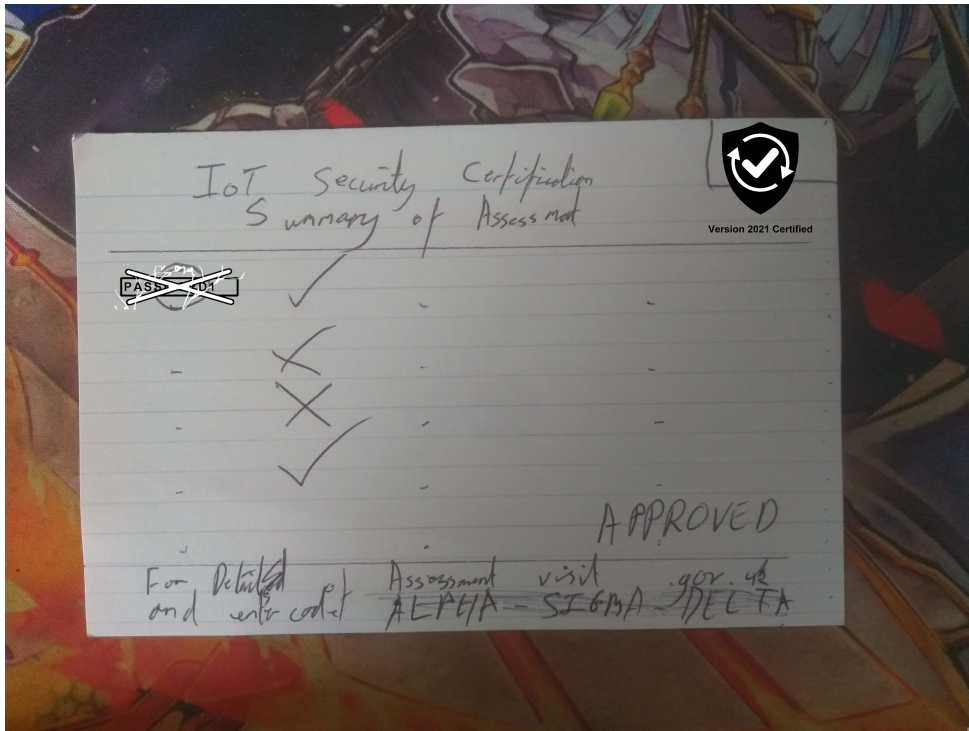


Figure 6: Label Paper Concept, created during discussions with artist

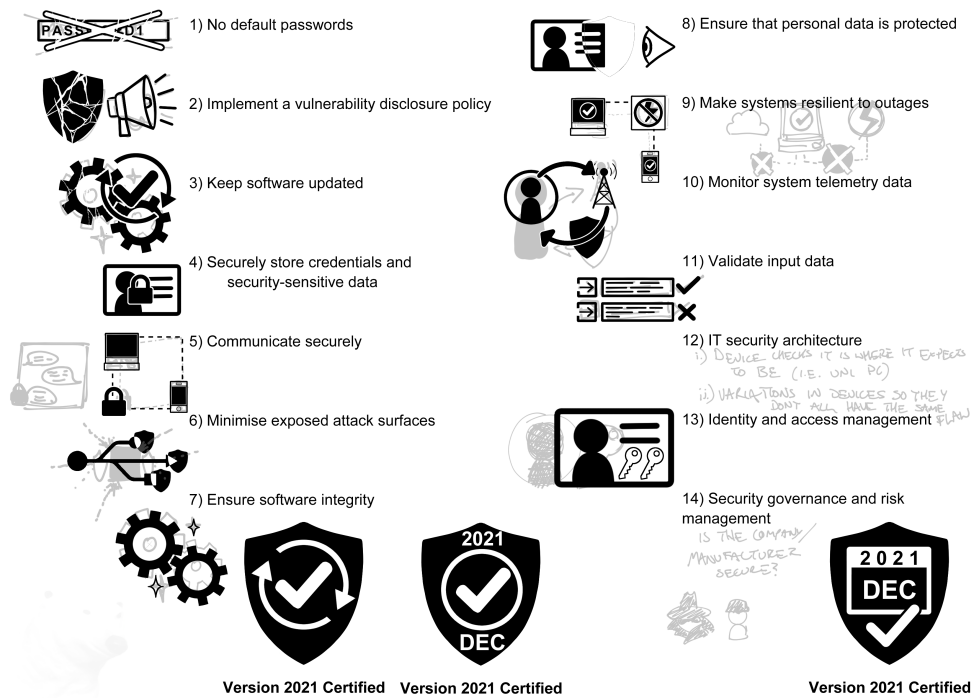


Figure 7: Figure depicting the initial Label Icons, after the first design session

The Design of each icon in Figure 7 was a collaborative effort with a commissioned artist, with rapid iterations of imagery. Themes, feelings and emotion fed into the design, such that the art should direct user attention in specific manner. Existing themes were incorporated (such as the recurring Shield icon, for Defence, Protection) and new themes established (Person to represent a User, an Identity. Cogs represent The System, Functionality, Action/Reaction.)

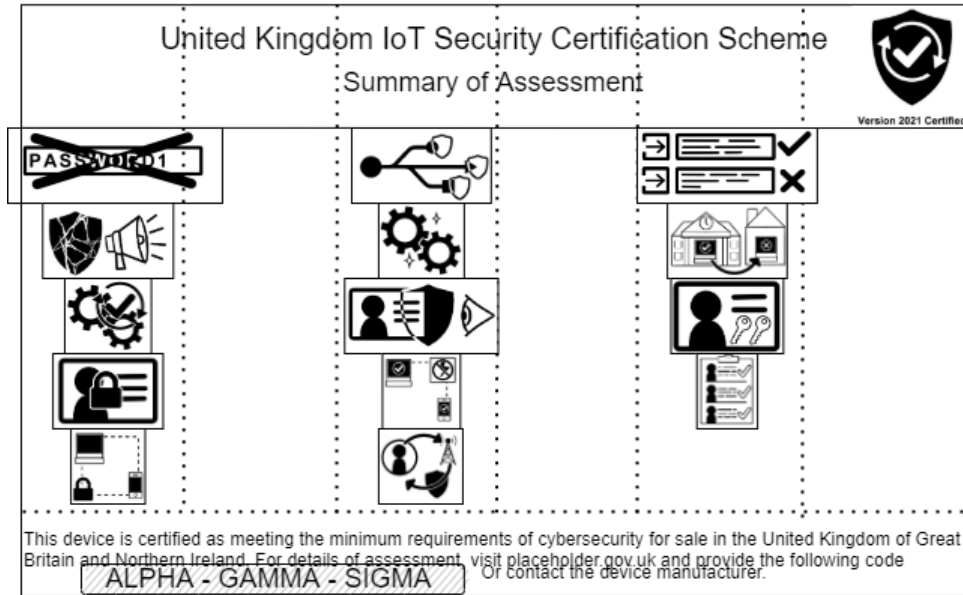


Figure 8: Label First Draft, with calculated spacings visible

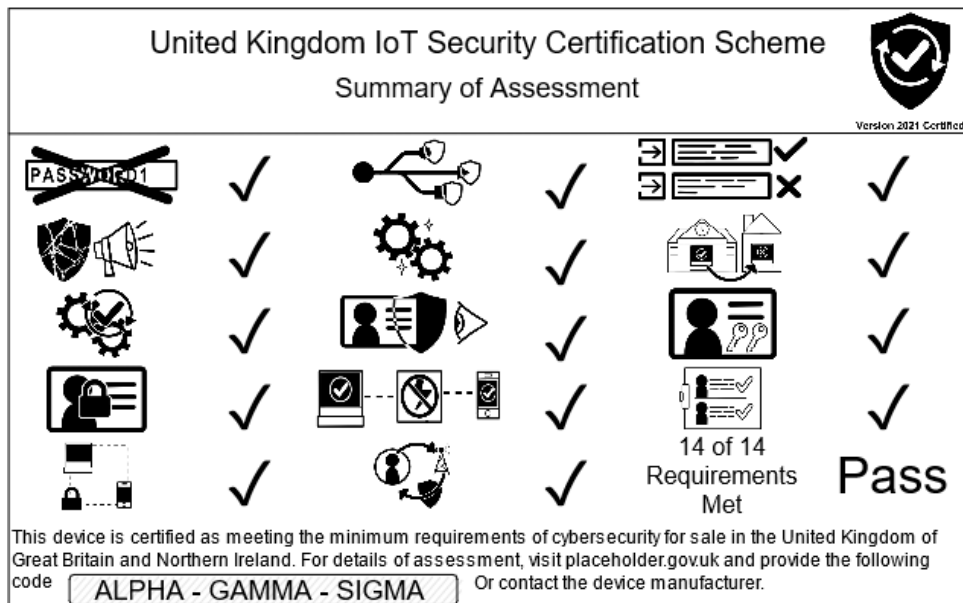


Figure 9: Draft Label with example certification, and spacings hidden












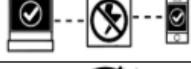



United Kingdom IoT Security Certification Scheme					
Summary of Assessment					Version 2021 Certified
	✓		✗		✗
	✓		✗		✗
	✓		✗		✗
	✗		✗		✗
	✗		✗	3 of 14 Requirements Met	<b>Pass</b>
This device is certified as meeting the minimum requirements of cybersecurity for sale in the United Kingdom of Great Britain and Northern Ireland. For details of assessment, contact the device manufacturer or visit placeholder.gov.uk and provide the following code:					
<b>ALPHA - GAMMA - SIGMA</b>					

Figure 10: Prototype design, carried forward to testing.

# 11 Prototype testing

As mentioned in subsection 9.3.3, the scale of testing has had to be reduced due to the Covid-19 pandemic. However, effort has been made to prevent the elimination of horizontal diversity of data sources. Instead, scale backs are in the quantity of samples for each source. This decision has been made as diverse sources of information are more likely to expose the kinds of weaknesses expected from a first prototype, which may be missed with a single homogenous source of information. Were future works to be undertaken that are funded for larger scale studies, these samples should also disincentivise high-quantity single-source methods which are usually prevalent in science (but can often miss the mark on usability).

## 11.1 User Studies

For user studies, the following were provided. These are three documents, expressed each in three formats for increased accessibility. As this study took place during Covid, the participants were recruited through University Adjacent social circles. A specific effort was made to ensure that the survey reached beyond computer-related disciplines and to ask for it to be shared into circles beyond the reach of University. It was still expected that the survey would struggle to reach other age groups (Covid isolation left no way to reach many age groups), so the decision was made to compress the scale of Cyber Security knowledge self-rating into the high end. This pre-emptive action would allow differentiation in results that otherwise would have been, perhaps, too compressed to distinguish.

### Summary of Results

From quantitative analysis of the data available, there are some prevalent correlated questions observable. Figure 11 highlights questions wherein there is a stronger correlation between answers with a darker shade of Green, whether positively or negatively associated. This correlation is not intended to be used as a statistical mechanism for analysis, but rather to shed light on the best locations to begin searching for hidden trends.

Of these starting points, one particularly strong negative correlation seems to be observable between the self-rated skill level and the desired size of a label. Those who are most proficient in Cyber Security matters prefer to receive less information. During analysis of Focus Group answers later, a potential cause for this relation is determined, wherein it seems those most proficient in Cyber Security underestimate the ability of others to comprehend a larger label, and as such desire a smaller label for the sake of others. A specific excerpt from the Cyber Professionals Focus Group follows

“(When discussing complex versus simple labels. For context, figure one is a small simple label, figure two is a more detailed version. Note how the Cyber Professionals desire figure two, yet are speaking for another group and advocating figure one) 00:09:25 Speaker 2 Er, I feel like figure one is more useful for just like the average person trying to buy off the shelf just because having the number, of having the data obvious is easily the most important information. ... 00:09:51 Speaker 5 Problem is, we’re looking at this as cyber security professionals and for us obviously the right hand side is going. 00:09:56 Speaker 5 To be more detailed. 00:09:58 Speaker 5 We can tell nearly exactly what it is. You know, there’s no exact headings or anything, but you could look up and check what these symbols 00:10:06 Speaker 5 Mean. Left-hand side? Yeah, I agree with ;Speaker 2;. 00:10:09 Speaker 5 The the general public is more likely to do a quick glance. Oh look that stickers on there cool, ticks ticks the box. Take that home. 00:10:19 Speaker 5 But yeah, me personally figure two. ... 00:10:33 Speaker 4 From like a product perspective, looking at B would find that far more useful.

”

Meanwhile, those who self-rate as less knowledgeable about Cyber Security have exhibited little issue comprehending the larger label, and consistently express a desire for even more information. When analysing survey answers, 86.36% found figure two more useful for making purchasing choices when Cyber Security was a concern. Almost three-quarters (72.73%) found it actually easier to understand this figure too, and 90.91% would rather see that label implemented. The author would like to remind the reader that these respondents were viewing the prototype labelling; significant improvements to the label have been made from the feedback gathered during that same survey, which directly address some of the reasons the remaining Negative respondents gave for their decision.



	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q13	Q14	Q15	Q16	Q18	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Age	Calibration	Q10	Q11	Q12	Q17	Q19		
Q1	1.00																																			
Q2	0.05	1.00																																		
Q3	-0.05	0.05	1.00																																	
Q4	-0.05	0.05	-0.05	1.00																																
Q5	-0.07	0.05	-0.07	0.69	1.00																															
Q6	-0.08	0.02	0.55	0.55	0.53	1.00																														
Q7	-0.07	0.07	0.69	0.69	0.46	0.80	1.00																													
Q8	0.55	0.09	-0.09	-0.09	-0.13	0.52	1.00																													
Q9	-0.11	0.11	0.46	-0.11	0.25	0.05	-0.15	1.00																												
Q13	-0.18	0.18	0.26	0.26	0.37	0.53	0.21	0.38	1.00																											
Q14	-0.05	0.05	-0.05	1.00	0.69	0.36	0.55	0.69	0.55	1.00																										
Q15	0.20	0.24	0.20	-0.24	-0.37	-0.06	0.10	-0.03	0.36	0.18	1.00																									
Q16	-0.09	0.09	0.55	0.55	0.79	0.65	0.61	0.79	-0.17	0.49	0.49	1.00																								
Q18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00																							
Q20	-0.09	0.09	-0.09	-0.09	0.33	0.05	-0.15	-0.13	-0.15	0.15	0.21	-0.09	-0.17	1.00																						
Q21	-0.09	0.09	0.55	0.55	0.79	0.65	0.61	0.80	-0.15	0.50	0.48	-0.17	0.55	0.48	1.00																					
Q22	-0.09	0.09	0.55	0.55	0.79	0.65	0.61	0.80	-0.15	0.50	0.48	-0.17	0.55	0.48	1.00																					
Q23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00																				
Q24	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00																			
Q25	-0.12	0.12	0.46	0.40	0.20	0.40	0.23	0.59	-0.22	0.01	-0.01	0.40	0.28	0.41	0.00	-0.22	0.42	1.00																		
Q26	-0.15	-0.32	-0.15	0.32	0.15	0.02	0.30	0.12	-0.27	-0.34	-0.17	0.32	0.04	0.04	0.00	0.01	0.01	0.01	1.00																	
Q27	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00																
Q28	-0.20	0.20	0.24	0.24	0.02	0.06	0.17	0.35	0.17	0.32	0.35	0.24	-0.08	0.16	0.00	0.00	0.00	0.00	0.00	0.00	1.00															
Q29	-0.20	0.20	0.24	0.24	0.05	0.26	0.17	0.35	0.10	0.32	0.35	0.24	-0.08	0.16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00														
Q30	-0.20	0.20	0.24	0.24	0.34	0.47	0.17	0.35	0.10	0.32	0.35	0.24	-0.08	0.16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00													
Q31	0.15	0.29	0.15	0.15	0.23	0.25	0.03	0.24	0.03	0.38	0.44	0.18	0.31	0.29	0.00	0.30	0.30	0.30	0.30	0.30	0.30	0.30	1.00													
Q32	-0.26	0.26	0.18	0.18	-0.08	0.09	0.05	0.26	0.06	0.18	0.13	0.18	0.17	0.04	0.00	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	1.00												
Age	0.10	-0.10	0.00	-0.48	-0.28	0.02	-0.15	-0.26	-0.19	-0.28	-0.09	-0.48	0.52	-0.15	0.00	0.19	-0.16	-0.16	-0.16	-0.16	-0.16	-0.16	-0.16	1.00												
Calibration	-0.30	-0.11	-0.02	0.58	-0.03	-0.20	0.28	0.26	-0.21	-0.28	0.02	-0.38	-0.12	-0.05	0.00	-0.05	-0.04	-0.04	-0.04	-0.04	-0.04	-0.04	-0.04	1.00												
Q10	-0.36	-0.18	-0.48	0.18	0.28	-0.22	-0.22	-0.22	-0.62	-0.32	0.12	0.18	-0.62	-0.05	0.00	0.18	-0.08	-0.08	-0.08	-0.08	-0.08	-0.08	-0.08	1.00												
Q11	-0.36	-0.02	0.02	0.30	0.10	-0.03	0.10	0.24	-0.02	0.14	0.20	0.30	-0.25	0.11	0.00	0.48	0.10	0.10	0.10	0.10	0.10	0.10	0.10	1.00												
Q12	-0.19	0.00	-0.19	-0.19	-0.10	-0.20	-0.35	-0.27	-0.22	0.00	-0.03	-0.19	0.03	-0.19	0.00	0.08	-0.20	-0.20	-0.20	-0.20	-0.20	-0.20	-0.20	1.00												
Q17	0.30	0.23	-0.23	0.04	-0.16	-0.27	-0.10	-0.14	0.55	-0.06	-0.20	0.04	0.18	-0.26	0.00	-0.26	-0.26	-0.26	-0.26	-0.26	-0.26	-0.26	-0.26	1.00												
Q19																									1.00											

Figure 11: Correlations between answers to questions (Larger Version and Data are available in appendices, within the spreadsheet survey-stats). If viewing digitally, this figure is full resolution and can be zoomed. Used to find potential areas to begin investigation, this is a table that shows questions that seem to have predictably related answers. For example, both question 22 and 23 seem to be strongly related to the answer within question 8. Both strong positive and negative relation are highlighted.

In almost all questions, a clear “favourite” answer was visible. However, true universal consensus was rare and there was at least one answer displaying characteristic anomalous to the calculated group answers. These deviant/anomalous answers are noted below, grouped by the user who expressed the answer. Additionally, “miss” answers are included, even if they were the majority opinion (a “miss” refers to an answer which indicates there may be some improvement or alteration desired, as the result is not what would have been hoped for in a perfect label.). Of significant interest is that surveys 1 and 20 both scored poorly for their initial impressions of the label, so close attention has been paid to their answers, in the hopes of determining potential causes. With both anomalous and “miss” answers included, it is hoped patterns may be visible.

User 1) Scored poorly in initial impressions of prototype label. An outlier with a low self-rated skill level wanting a smaller label. 50% miss for ‘understanding’ criteria. Miss for usability in general and worked example. Preferred a simpler example.

User 3) Most compact label desired. However, was able to complete the provided exercise and no significant difficulties were observed. Perhaps the high skill level was their reasoning for desiring a compact label, not any personally experienced difficulties?

User 5) Significantly above expected average skill level. Desires more compact label. However, was able to complete exercise and no significant difficulties observed. Perhaps the high skill level was their reasoning for desiring a compact label, not any personally experienced difficulties?

User 9) Significantly above expected average skill level. Desires more compact label. However, was able to complete exercise and no significant difficulties observed. Perhaps the high skill level was their reasoning for desiring a compact label, not any personally experienced difficulties?

User 12) High skill level. No other deviations observed.

User 13) Didn’t complete worked example. Desires larger label with more explanation. Perhaps why they were not able to complete the example?

User 15) High skill level. No other deviations observed.

User 19) Significantly above expected average skill level. Concerns expressed in initial impressions. Miss for usability in general and worked example. Preferred a simpler example. Perhaps the high skill level was their reasoning for desiring a compact label, not any personally experienced difficulties?

User 20) Scored poorly in initial impressions. 75% miss on understanding. Miss for usability in general and worked example. Preferred a simpler example.

There were many areas in the User Studies designated with free-comments, for the purpose of gathering qualitative data. With user studies, an unfortunate limitation is that your questions are pre-written before the users have had any chance for input. This can unintentionally result in the researcher excluding an area with valuable and unexpected insights. Included are unique identifiers for each respondent, such that readers may try to observe/verify patterns themselves (these are the same identifiers from prior sections).

Here follows analysis of answers for each free-use question. Justification that allowing so many free-form answers was correct is clearly visible here, as almost all yield some valuable insight that would have not been otherwise picked up, enhancing the development of this label prototype.

Question 1) Comments suggest that the label A is interpreted as having a high level of security (or conversely, that label B conveys a low level of security). There are some expressions that label A is vague (participants 5, 7, 11, 14, 15, 17, 18).

Question 9) Figure Four is described frequently (1, 7, 8, 12, 13, 15, 20) as confusing, however, the commenters themselves state this would be remedied by explanations of the symbols (which is already on-spec), so this has not been raised as a concern. (2, 14) describe a feeling of uniqueness to Figure Four, that it is tailored to each product, whereas figure three conveyed a feeling of being copied and pasted to many products. This feeling is echoed in 5, with description of thought going into the certification of the device. This feeling of uniqueness is not something intended, but something that can be noted and leveraged, as a feeling of copy-paste is stated as making the commenters more likely to ignore the label (“it is a much more detailed label which is unique to each device compared to the left one which can be copied and pasted to any product without a thought”, participant 2).

Question 20) Almost all comments convey a feeling of uneasiness at the proposed state of the security requirements. However, a few comments focus on the bright side that there is at least a proposed minimum (3, 16, 18). Not much useful insight otherwise, just affirmation that consumers are disappointed by current cybersecurity strategies and planned mitigations.

Question 21) There is a lot of reinforcement about what was raised in Q9, that accompanying information is needed. An obvious alteration that was somehow missed is suggested (10); The requirements are currently not numbered. Therefore, “Requirement 3” could be interpreted as multiple different requirements. This will also help with looking up the information online. There is additionally a comment (11) about symbol consistency, that they have different aspect ratios and resolutions. This issue is something that can easily change were the suggestions of this report implemented; these prototype designs should not be taken as a “finished result”.

Question 28) Vague tones of agreement; little useful information otherwise.

Question 29) Lots of comments asking for the information from earlier label design to come back (3, 4, 5, 7, 10, 11, 15, 17). Many “passionate” responses, showing the respondents valued the prior information highly.

Question 30) Further requests for the lost information (2, 3, 4, 5, 7, 9, 13, 14, 17).

Question 31) Support shown for the new minimal lozenge (4, 14).

Question 32) Various suggestions, no particular patterns identifiable in the responses, due to the uniqueness of each answer.

## **11.2 Focus Group Interviews**

Two different groups knowledgeable and with express qualification in the Cyber Security Sector were interviewed separately to gather additional feedback; those working professionally in a Cyber Security context, and those engaged in Cyber-Related Research at Swansea University. Before the interview/focus-group commenced, they were distributed a Consent Form, Fact Sheet and Assistive Questionnaire in ODT and DOCX format. Of notable difference from the Survey, the PDF is omitted. This change is because it was desired by the author to encourage note taking on the document. This could be done in artificial white space added, to avoid “spoilers” of upcoming questions, while doubling as space for longer form answers.

Additionally, while the Questions document is (other than the aforementioned white space) nearly identical to that used for the Survey, the procedure was different. Questions were not to be answered privately, but to be launching points for discussion as a group. Answers themselves were not recorded (as this was not a survey), but instead the discussion was where value was to be extracted.

The Consent Form, Fact Sheet and Assistive Questionnaire distributed to the Focus Group participants was identical for both Cyber Professionals and Cyber Academics; They are located in the appendices here section 16

### **11.2.1 Cyber Professionals**

The Cyber Professionals group were gathered from a known pool of contacts worldwide, who were invited to participate. While individual profession varied, the group was composed entirely of individuals who currently work/have recently worked within or in close proximity to the UK Cybersecurity Sector.

This focus group were vigorous in their discussions, with enthusiasm that is invisible through the transcription. Audio Channels were captured separately due to anticipated crosstalk, which allowed every answer to be heard clearly when processing the feedback. Total recorded discussion lasted one hour and thirty-three minutes, with talk of many edge cases and potential considerations to ensure the robustness of the proposed labelling system.

A particular example of testing this robustness is that of the hypothetical IoT Toothbrush. Challenging aspects of the label such as invalidity of entire requirements, components of requirements, even deliberately subversion through engineering devices to receive higher scores than they should otherwise have been entitled to. Through this process, several important adjustments and clarifications have been made (detailed in section 11.2.2) particularly around how to respond to invalid requirements.

### **11.2.2 Cyber Academics**

Audio Channels were captured separately due to anticipated crosstalk, however this was not needed due to the relatively slow-paced discussion that occurred. The total recorded session lasted 32 minutes. Unfortunately, despite the efforts of participants, this session was unedifying and most discussion points had already been covered. As opposed to inspired discussion, answers fell in expected bounds of a normal privately-filled survey and suggestions were similarly basic. A notable exception to this is the suggestion of a QR code, which had unfortunately already been excluded for reasons discussed in subsection 4.1. This being said, the data gathered here reaffirms the validity of data collected from the Surveys by falling in similar bounds despite a different method of data collection.

### **Summary of Changes**

Numbering: The individual requirements shown on the label need numbering for the label to make sense.

Add a date updates are until: A simple addition, taken from the simplified labels into the mainline proposal.

Short text description instead of whitespace: While the second-layer descriptions are useful, having at least a refresher description will aid in recall (a thousand pictures can be less useful than a single word!s)

Invalid Requirements “Not Applicable”: Specify how requirements should handle excluding features or hardware, with specific intent to limit adversarial designs by manufacturers.

Grade A-F instead of Pass fail: Fine grained grading allows for a gradient, to express increasingly subtle distinctions between differing device requirements.

Add numeric x of y instead of tick cross: Incentivise improvement above the baseline for a “grade” by crediting sub-requirements, through an “x of y” subrequirements met.

A lot of discussion around further revision of the standards. Revisions are something that would have to be discussed with industry extensively, but some key refinements include colour grading (what counts as good/okay/bad and the bounds for each would need to be established) as well as expanding an A to F grading system to require certain key points to be covered, as well as a number of “pick and choose”. To account for non-applicable, this may mean that the sub-components themselves of each requirement have to be revised (A work more for agencies than individuals).

## 12 Revised Label Specification

After incorporating the changes from the Survey results and the focus groups, the following is the new format for the label.

Version 2021 Certified		United Kingdom IoT Security Certification Scheme				Updates Until Dec 2024	
Summary of Assessment							
	1: 6/6		6: 8/8		11: 9/9		
	2: 6/6		7: 10/10		12: 2/2		
	3: 7/7		8: 11/11		13: 2/2		
	4: 5/5		9: 4/4		14: 3/3		
	5: 10/10		10: 6/6	14 of 14 Requirements Met <b>Pass</b>			
This device is certified as meeting the minimum requirements of cybersecurity for sale in the United Kingdom of Great Britain and Northern Ireland. For details of assessment, contact the device manufacturer or visit placeholder.gov.uk and provide the following code: <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-top: 5px;"> <b>ALPHA - GAMMA - SIGMA</b> </div>							

Figure 12: Revised design, following feedback from prototype. The label now includes Numbering of Requirements, a date for when updates are guaranteed until, and a x/y for each requirement that illustrates how many subrequirements have been met (with colouration to indicate a good or bad result)

This particular configuration would work without any of the changes from future works, and (with the rest of the works outlined in the report) function stand-alone. Not shown in this example, but included in the proposal, is the support for Not-Applicable requirements (which will be greyed out, and subtracted from x of 14 requirements met. A single N/A requirement would give 13 of 13 requirements met). A failed requirement (IE where the minimum specified requirements for certification were not met) will be shaded Red instead of Green. Note that, due to the fact that fine-grained information of which specific sub-requirements is only available in the detailed online report, a particular weakness of this design is that confusing situations can occur where 6/7 requirements are met but fail. The inverse can occur too, where 1/7 sub-requirements pass but the category still meets the minimum. This abnormality occurs because the passing of a requirement is determined by meeting certain specific sub-requirements, and that information is not visible on the product label. The following example showcases some of these behaviours.

Version 2021 Certified		United Kingdom IoT Security Certification Scheme										2024 DEC	
Summary of Assessment													
	1:	5/6		6:	8/8		11:	8/9					
	2:	2/6		7:	9/10		12:	2/2					
	3:	7/7		8:	1/11		13:	N/A					
	4:	5/5		9:	4/4		14:	1/3					
	5:	10/10		10:	6/6	11 of 13 Requirements Met <b>Pass</b>							
This device is certified as meeting the minimum requirements of cybersecurity for sale in the United Kingdom of Great Britain and Northern Ireland. For details of assessment, contact the device manufacturer or visit placeholder.gov.uk and provide the following code: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td><b>ALPHA - GAMMA - SIGMA</b></td> </tr> </table>													<b>ALPHA - GAMMA - SIGMA</b>
<b>ALPHA - GAMMA - SIGMA</b>													

Figure 13: Revised design, showing further features from the prior figure. Visible now is how a Non-Applicable result could be displayed, as well as failed requirements.

While the configuration would work stand-alone, it has also been outlined how future works may be incorporated into this template in a manner that would vastly strengthen the proposal]. Figure 14 is visually similar to the prior label, but the inclusion of colour gradient (as opposed to binary pass/fail colouring) as well as Grading (Mocked as A-F, but other scales can substitute) requires the existence of the future work outlined in subsection 14.3. Agreed meaningful sub-categorisations, based on real industry collaborations, are necessary to create finer boundaries than “Pass/Fail”. The following illustrates a simple adaptation of the label that works with such changes.

United Kingdom IoT Security Certification Scheme					2024 DEC	
Summary of Assessment						
Version 2021 Certified					Updates Until Dec 2024	
	1: 5/6		6: 8/8		11: 9/9	
	2: 2/6		7: 10/10		12: 2/2	
	3: 3/7		8: 11/11		13: N/A	
	4: 5/5		9: 4/4		14: 3/3	
	5: 10/10		10: 6/6	12 of 13 Requirements Met		Grade B
This device is certified as meeting the minimum requirements of cybersecurity for sale in the United Kingdom of Great Britain and Northern Ireland. For details of assessment, contact the device manufacturer or visit placeholder.gov.uk and provide the following code: <b>ALPHA - GAMMA - SIGMA</b>						

Figure 14: Revised design, showing further features from the prior two figures. A passed requirement is shown, but in the colour Orange, to indicate caution. This is because although the device met the minimum required, the majority of results in that category are still a fail

Figure 15 is the logical culmination of these future works, along with the feedback gathered throughout this project. This can be considered the final form, and “best” case that could emerge.

United Kingdom IoT Security Certification Scheme					2024 DEC	
Summary of Assessment						
Version 2021 Certified					Updates until Dec 2024	
 Password Protections	1: 5/6	 Reduced Attack Surface	6: 8/8	 Data Validation	11: 9/9	
 Vulnerability Disclosure	2: 2/6	 Device Integrity	7: 10/10	 Security Architecture	12: 2/2	
 Device Updates	3: 3/7	 Protect Personal Data	8: 11/11	 Access Management	13: N/A	
 Credential Storage	4: 5/5	 Outage Resilience	9: 4/4	 Risk Management	14: 3/3	
 Communicate Securely	5: 10/10	 Monitor System Data	10: 6/6	12 of 13 Requirements Met		Grade B
This device is certified as meeting the minimum requirements of cybersecurity for sale in the United Kingdom of Great Britain and Northern Ireland. For details of assessment, contact the device manufacturer or visit placeholder.gov.uk and provide the following code: <b>ALPHA - GAMMA - SIGMA</b>						

Figure 15: Final Label, with all extended features and future works included

The second layer of this proposed system has rarely been visualised in this report, as actual design of all government websites is strictly controlled, with a consistently accessible design. It is more useful to create a feature list, as how this will actually be visualised is a variable with little control. However, at this stage, some primitive mock-ups have been included as a visual aid. Again, this is not how any actual design would appear, the mockups are simply a visualised feature list.

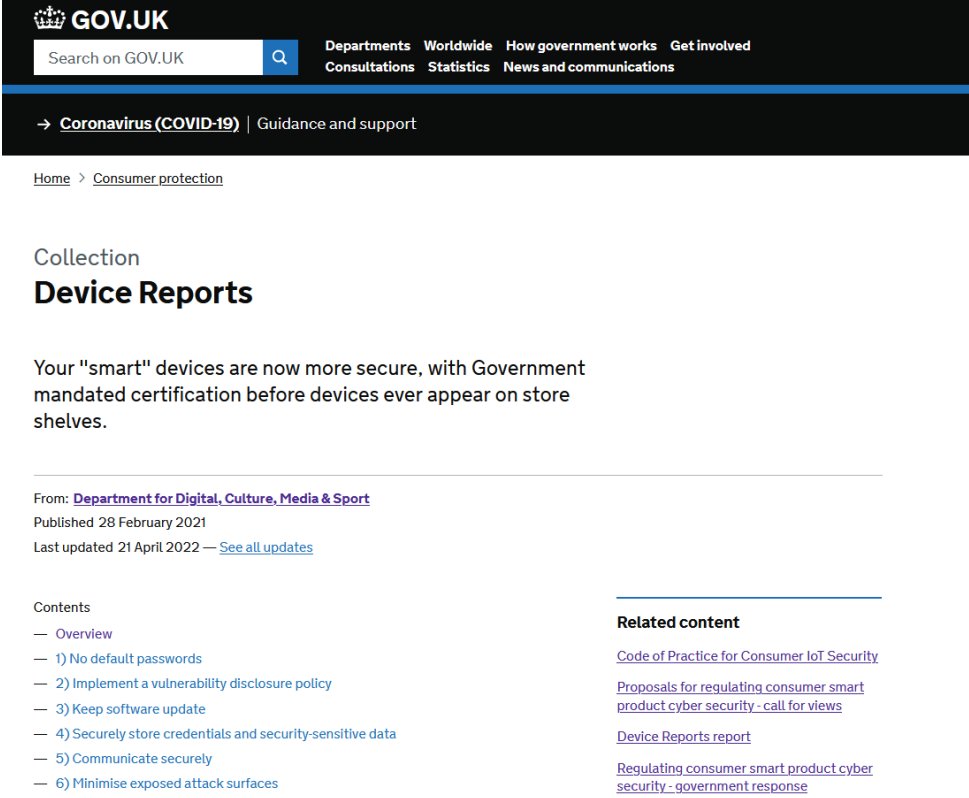


Figure 16: General Landing Page when looking up the scheme, styled as a GOV website, and following their known design requirements

As best as can be attempted, Figure 16 is a mock-up in the styling of a GOV website, to illustrate the restrictive nature of the design. This figure is an example of what the landing page for general information on the scheme may look like.



## Device Reports


Every "smart" device certified for sale in the United Kingdom has undergone a security assessment, to help our citizens remain safe and secure in a digital world.


While a brief summary is visible on product packaging, the full report with complete descriptions of how the device performed is available free online. To access this, simply enter the three-word code on the rear packaging of the device into the following box.

For instructions on finding this code, click or tap any of this text.

—  —

Alternatively, you may search by device name to find a specific report you wish to view.

Amazon Alexa 2021  
  
Device Image

Amazon Alexa 2020  
  
Device Image


Amazon Alexa 2019  
  
Device Image

Figure 17: Mockup of finding a specific device using the GOV website, where the three-word-code can be entered or a device discovered by name

Now moving into mock-ups of features, Figure 17 is specifically a lookup page for devices. Three boxes exist, for entering the code from the back of the box (the cursor should automatically move to the next box upon completion of a word, such that people don't try to enter the dash). Potential customers may wish to view a report before physically having access to a device, so a search feature is included. Advanced search features should be included, to help differentiate devices by many different characteristics (as can be seen in the example, it could be hard to differentiate differing year editions of devices without this). Important considerations are to include device pictures in-line with the search, to help with correct identification early. The most recent editions of devices should also be displayed first, as those are the most likely to be on store shelves. If a customer is unable to immediately see their desired device, they may simply get frustrated and click any, as opposed to searching through to find the exact match.

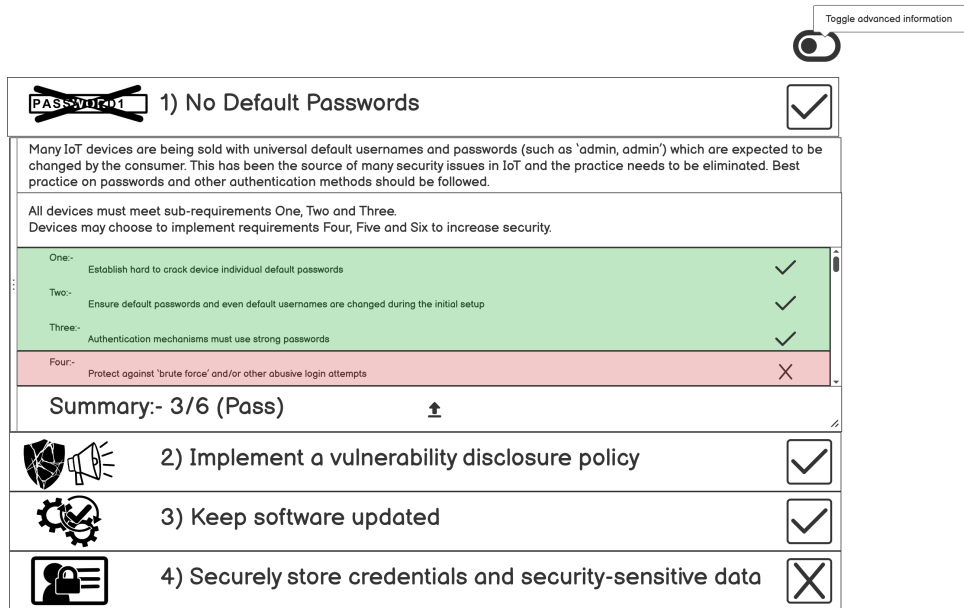


Figure 18: Mockup of a Device Report, as a consumer would see. Expandable sections are visible, with detailed information on this device, the requirements it both passed and failed. An advanced information toggle is set to off.

Figure 18 is a mock-up of the detailed report for a specific device, that a customer may view. The first category has been clicked and expanded, to show a simple description of what that requirement entails. Also visible are the individual simple descriptions of each sub-requirement. As a user has taken an interest in the detailed report by searching this, the information they are first greeted with should be as accessible and simple as possible. This reasoning is why the technical specification is hidden behind a toggle for Advanced Information.

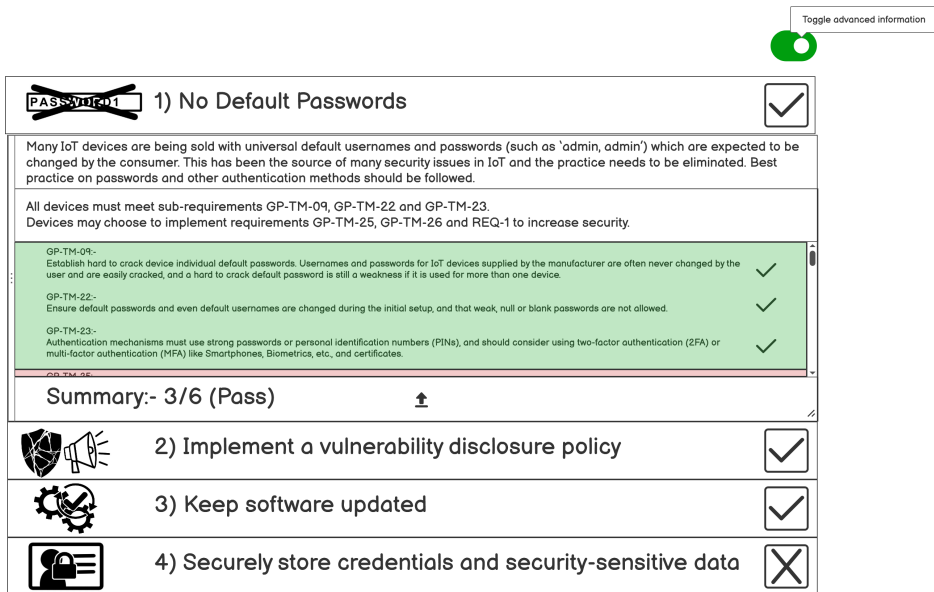


Figure 19: Mockup of a Device Report, when Advanced Information visibility is enabled. Opposed to the prior figure, Advanced Information is now visible, which shows the Policy Codes for the requirements, as well as their full technical description.

Displaying how the technical definitions differ from their simplified versions, Figure 19 displays the same report with the Advanced Information toggle enabled.

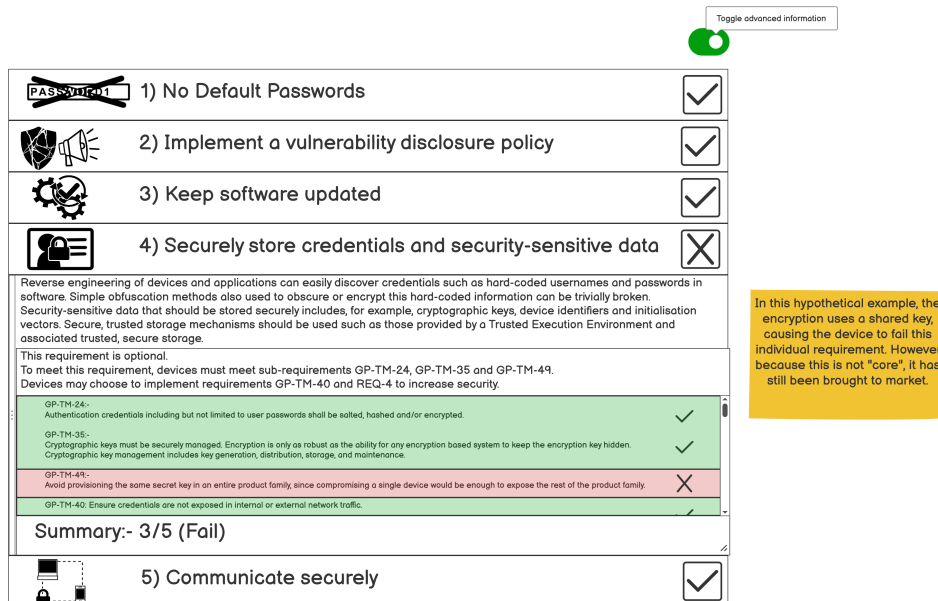


Figure 20: Mockup of a Device Report, when Advanced Information visibility is enabled

Another view of the same interface and report, to show how a failed requirement is conveyed. This interface is a hypothetical, where the "Includes" requirements are mandatory for a pass in every requirement.

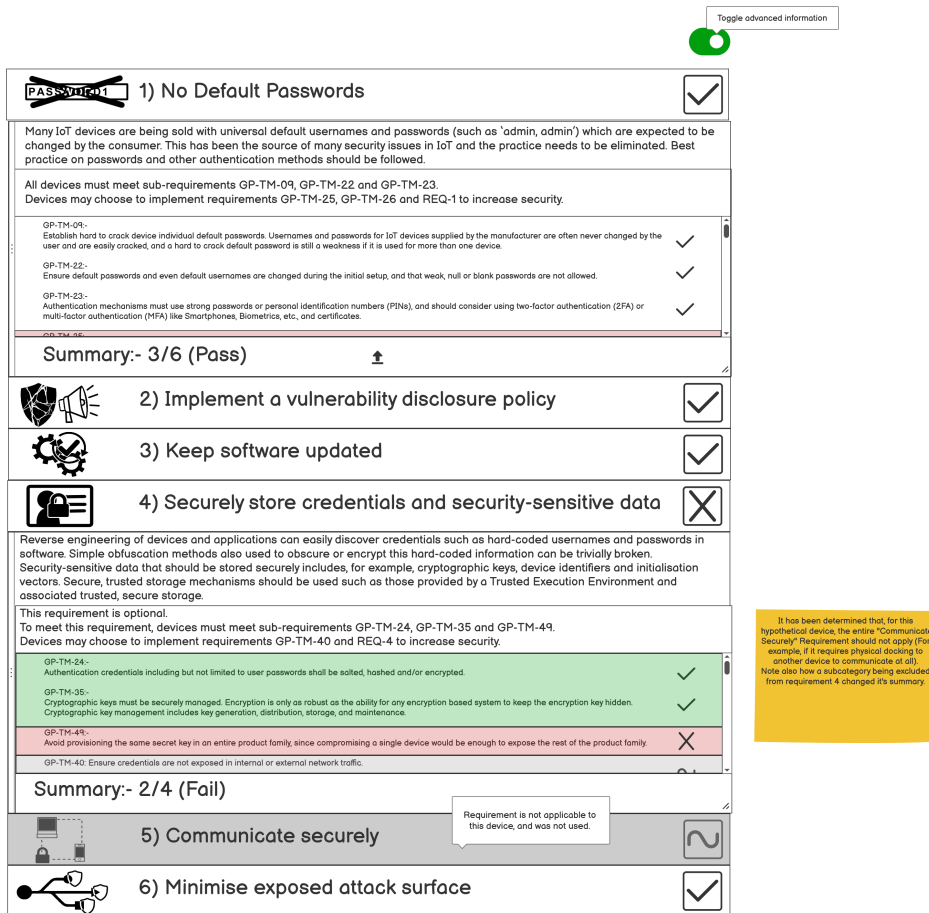








Figure 21: Mockup of a Device Report, with Further Work integrated

Building further from this hypothetical, device assessments should also have a Not-Applicable option. As shown, these are removed entirely and do not effect a device assessment in any way. Additionally, limited agreements and collaborations with industry (outlined in future work) could allow for passes to come from “must contain x of y”, as shown in this requirement four. Many are shown expanded, but this figure is just for demonstration, and only a single category should be expandable at a time.

	<b>1) No Default Passwords</b>	<b>C</b>
<p>Many IoT devices are being sold with universal default usernames and passwords (such as 'admin, admin') which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed.</p> <p>All devices must meet sub-requirements GP-TM-09, GP-TM-22 and GP-TM-23. Devices may choose to implement requirements GP-TM-25, GP-TM-26 and REQ-1 to increase security.</p>		
<p>GP-TM-09- Establish hard to crack device individual default passwords. Usernames and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked, and a hard to crack default password is still a weakness if it is used for more than one device. ✓</p> <p>GP-TM-22- Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed. ✓</p> <p>GP-TM-23- Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates. ✓</p>		
<p>Summary:- 3/6 (C)</p>		
	<b>2) Implement a vulnerability disclosure policy</b>	<b>A</b>
	<b>3) Keep software updated</b>	<b>A</b>
	<b>4) Securely store credentials and security-sensitive data</b>	<b>D</b>
<p>Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys, device identifiers and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment and associated trusted, secure storage.</p> <p>This requirement is optional. To meet this requirement, devices must meet sub-requirements GP-TM-24, GP-TM-35 and GP-TM-49. Devices may choose to implement requirements GP-TM-40 and REQ-4 to increase security.</p>		
<p>GP-TM-24- Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted. ✓</p> <p>GP-TM-35- Cryptographic keys must be securely managed. Encryption is only as robust as the ability for any encryption based system to keep the encryption key hidden. Cryptographic key management includes key generation, distribution, storage, and maintenance. ✓</p> <p>GP-TM-49- Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family. ✗</p> <p>GP-TM-40- Ensure credentials are not exposed in internal or external network traffic.</p>		
<p>Summary:- 2/4 (Fail)</p>		
	<b>5) Communicate securely</b>	<b>2</b>
<p>Requirement is not applicable to this device, and was not used.</p>		
	<b>6) Minimise exposed attack surface</b>	<b>E</b>
<p>All devices and services should operate on the 'principle of least privilege', unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.</p> <p>This requirement is optional. To meet this requirement, devices must meet sub-requirements GP-TM-33 and GP-TM-50. Devices must additionally include two of the following to pass. GP-TM-30, GP-TM-45, GP-PS-12 and REQ-6. Devices may choose to implement requirements GP-TM-33, GP-TM-50, GP-TM-08, GP-TM-43, GP-TM-45, GP-PS-12, GP-TM-30 and REQ-4 to increase security.</p>		
<p>GP-TM-33- Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections. ✓</p> <p>GP-TM-50- Ensure only necessary ports are exposed and available. ✓</p> <p>GP-TM-08- Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default. Strong security controls should be something the consumer has to deliberately disable rather than deliberately enable. ✗</p>		
<p>Summary:- 2/8 (Fail)</p>		

It has been determined that, for this hypothetical device, the entire "Communicate Securely" Requirement should not apply (For example, if it requires physical docking to another device to communicate at all). Note also how a subcategory being excluded from requirement 4 changed it's summary

Figure 22: Mockup of a Device Report, with additional Further Work integrated

Integrating future works, the ideal companion to the label would have fine-grained grading, as opposed to pass/fail. The extra tiers allow “devices must additionally include two of the following four”, as shown in requirement 6. This is the ideal “best case” result for features of a second-layer report, with the most available information while also not overloading the consumer (as the default is simplified).

## Part V

# Conclusions and Future Improvements

## 13 Summary

Within these works, the author has attempted to lay solid foundations for rapid advancement of security standards in the field of Internet of Things devices. To do this, an existing framework that was constructed to fill the legislative gap post-Brexit in the United Kingdom was taken as a starting point. After ensuring its foundations were solid through deconstruction of its requirements, recommendations of another organisation were merged in, to create a more robust framework. After some refactoring of the requirements, wherein some categories were created and others deconstructed, a small number of additional improvements were noted as being possible to add to this framework.

Recognising the potential of a plan to create a consumer facing label, the proposal expands to include additional desirable characteristics for a label. This was presented to a small group of consumers and two relevant focus groups, to ensure the proposal was fit for purpose. Feedback was integrated, and a final proposal has been put forth for a two-layer labelling system which can accommodate many potential variations of the underlying legislative framework.

## 14 Future Work

To aid others in building upon this work, here follow some recommendations for future work to develop a more secure future for the Internet of Things.

### 14.1 Mappings between Additional Security Standards

When this work was started, the only internationally recognised attempts at standardisation were the ENISA Baseline Security Requirements and the (at the time, in draft form) UK Secure by Design Requirements. Since then, not only have these contributors continued to evolve their offerings, but other market players have emerged. The IoT Cybersecurity Improvement Act of 2020 [176] in the United States declared that the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) were to take measures to improve IoT security. This manifested in NIST IR 8425, Profile of the IoT Core Baseline for Consumer IoT Products [177] which is another reference document for improving IoT security. The Australian Government released their own version of voluntary recommendations in 2020 [178] which seems heavily inspired by the UK Secure by Design proposal, and the IMDA of Singapore [179] launched a cybersecurity guide. It is expected that this will continue, with more and more worldwide governments putting forward their own vision of a more secure Internet of Things.

It is likely that, as was observed between the ENISA requirements and the UK requirements, that these (and other emerging standards) will have significant overlap. Creating mappings between these will allow translation and conversion of equivalent criteria, and expose any new improvement beyond the current known baseline. Particular care should be taken when determining “equivalent” criteria, to clarify if this is true equivalence. For example, viewing from the perspective of the UK Requirements, if requirement one were met then it could likely be stated that requirement one of the Australian proposal were also met and the closest ENISA equivalent would still require additional works. However, viewing from the perspective of ENISA requirements, meeting that closest equivalent would be in excess of both the UK and Australian proposals.

Expressing these relations in an easy to use interactive format (perhaps with known presets and pre-configurations) could be helpful for propagating IoT security requirements further than their jurisdiction. In the prior example of UK requirement one, the works to achieve equivalence with the ENISA requirements are relatively minor. Stakeholders may exceed local requirement with International requirements (and sales) in mind.

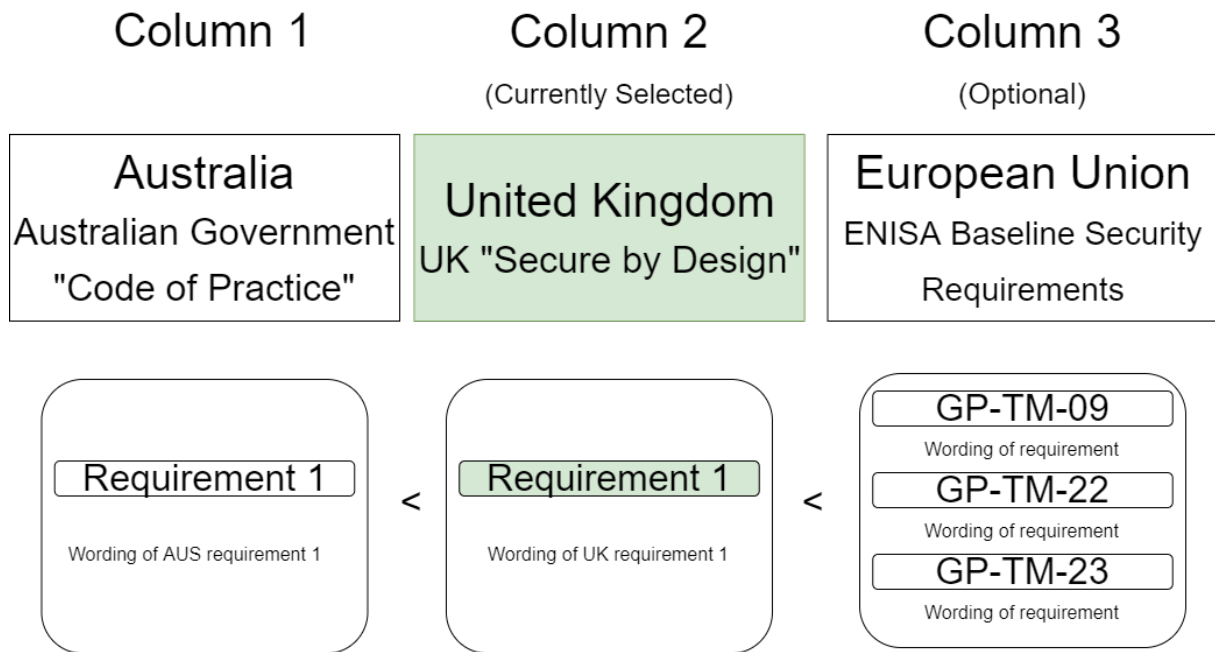


Figure 23: Example illustration of a potential version of mentioned Mapping Software

## 14.2 Further User-Based Research

Initial scoping for the User Studies had between 1e2 and 1e3 users. This was intended as a small scale test, but Covid-19 reduced this exponent. There is a case for not only repeating the existing testing with larger groups that sample across a wider populace, but also for expanding the testing itself into new areas.

Some significant justifications for further user studies are to provide a more representative sample of the population (many of the high age brackets were under self isolation and inaccessible for Covid during the testing), to have in-person focus groups with handheld prototypes as opposed to digital imagery, to run the same experiment (or similar experiment) with the much larger population to verify the collected results, or to run entirely distinct user testing from the author's own methodology, attempting to gather additional considerations.

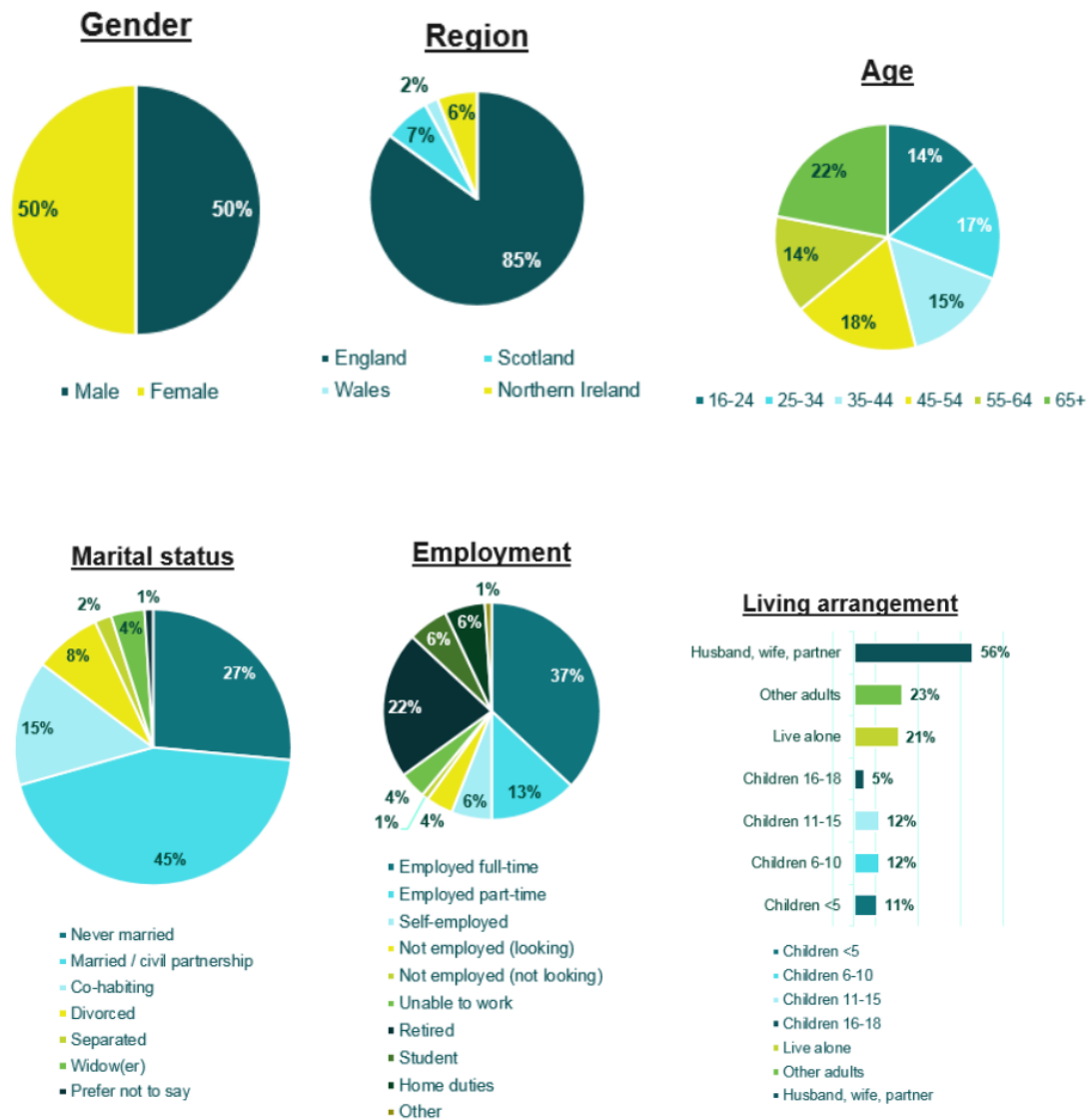


Figure 24: Partial demographic information from Harris Interactive Survey [58]

All prior attempts at user studies have at least attempted to weight responses according to UK demographics [58], however deviating from this can be easily justified. A wide-population survey may identify that those in specific demographic subgroups require deeper investigation (for example, perhaps an age cut-off is observed where the responses from participants became uninformative when attempting a generic user study). These deep dives can reveal additional information that would otherwise be diluted too far in a wide population survey, or just lost simply through the methodology. Harris Interactive may have balanced their demographics in proportion to the UK Census Results, but the surveys were filled out online. In a survey which involves understanding internet connected products at the point of sale, their method selectively screened out those who are most likely to experience difficulties understanding the products.



Caution should be taken when replicating other features common to surveys and other user based research. Primarily, excessive collection of information. In Figure 24 is a sample of the demographic information publicised by Harris Interactive for their participants. Collecting the information, solely for the purposes of ensuring the sample is representative of the UK population, is necessary. Collecting extra information with the intent of discovering relationships between data can also be justified, however the research runs the risk of accidental misrepresentation through P-hacking [180].

### 14.3 Subcategorisation based on external input

Recognised in Focus Groups particularly, and justified by the expanded discussions of edge-case IoT devices, is that much can be done in the way of sub-categorisation to enhance this work.

Each requirement currently consists of many subcomponents already, largely expressed as ENISA baseline security requirements. However, beyond the “category” they reside in, there is no other relationship between the requirements. Exploring different groupings and relations between subcomponents could take many forms that would benefit the standard.

ETSI provide a simple example that could be ported to the standard, rooted in wording. Within ETSI drafting rules [56], use of keywords such as “will”, “shall”, or “should” determine if a requirement must be followed or is optional. However, requirements can still inherit from others. This gives a logical structure similar to Figure 25.

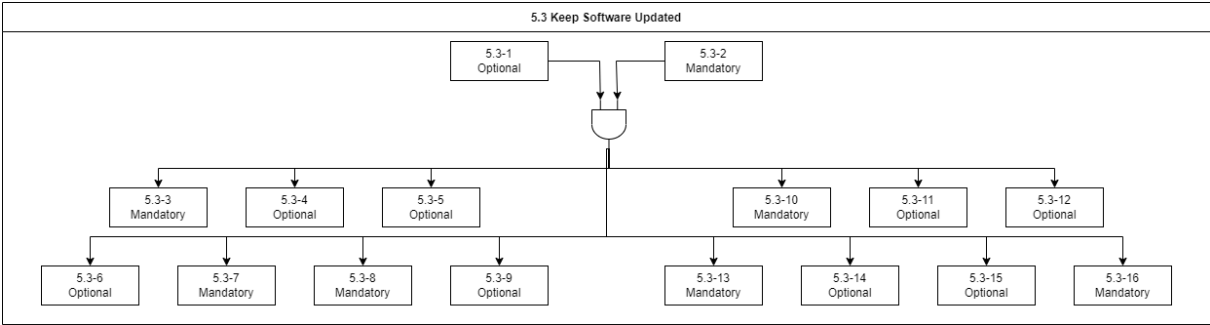


Figure 25: ETSI Requirement 5.3 logic diagram

This simple tree with just a single logic gate already helps to visualise quite a lot about how the standard could be improved through advanced applications. More complex works, with many “tiers” and logical connections **that are backed up by communication with industry** would be a valuable resource. This emphasis is important, as attempts at making these logical groupings were specifically excluded from this work, as without that external input the value which could be extracted would be disproportionately low compared to the works undertaken.

Some recommended configurations to try could be to weight for an A-F system, based on the European Energy Certifications. This system is recognisable and easy to work with, but having well justified boundaries may be difficult for so many divisions. Colour grading was another popular choice, with FAIL, red, orange, green. Despite worldwide cultural differences for such colours, that schema is well recognised in the UK (such that even those with colour-blindness are familiar enough and can distinguish the shades). A system that is less accessible to end users, but perhaps could generate the best justified groupings, would be for weighted graphs to determine grades and ratings for devices. It is easy to see Data Science fulfilling the demand for a strict empirical basis of boundaries, emerging where recommendations from different shareholders become irreconcilable.

## References

- [1] Fortinet. *What Is Operational Security? OPSEC Explained Fortinet*. 2022. URL: <https://www.fortinet.com/resources/cyberglossary/operational-security>.
- [2] Hannah Ritchie and Max Roser. "Age Structure". In: *Our World in Data* (2019). <https://ourworldindata.org/age-structure>.
- [3] Hannah Ritchie and Max Roser. "Technology Adoption". In: *Our World in Data* (2017). <https://ourworldindata.org/technology-adoption>.
- [4] Mariela Leibovich. "Proactive vs. Reactive Cybersecurity". In: *CYREBRO* (2022). URL: <https://www.cyrebro.io/blog/proactive-and-reactive-cybersecurity> (visited on 08/23/2022).
- [5] Wikipedia contributors. *Windows NT — Wikipedia, The Free Encyclopedia*. [Online; accessed 23-August-2022]. Aug. 23, 2022. URL: [https://en.wikipedia.org/w/index.php?title=Windows\\_NT&oldid=1105883114](https://en.wikipedia.org/w/index.php?title=Windows_NT&oldid=1105883114).
- [6] Geoff Chappell. *Kernel Versions*. 2021. URL: <https://geoffchappell.com/studies/windows/km/ntoskrnl/history/index.htm> (visited on 08/23/2022).
- [7] Jon Martindale. "From pranks to nuclear sabotage, this is the history of malware". In: *Digital Trends* (2018). URL: <https://www.digitaltrends.com/computing/history-of-malware> (visited on 08/23/2022).
- [8] Dan Ilett. "Hacking poses threats to business". In: *ComputerWeekly* (2007). URL: <https://www.computerweekly.com/feature/Hacking-poses-threats-to-business> (visited on 08/23/2022).
- [9] Scott Granneman. "Infected in 20 minutes". In: *The Register* (2004). URL: [https://www.theregister.com/2004/08/19/infected\\_in20\\_minutes](https://www.theregister.com/2004/08/19/infected_in20_minutes) (visited on 08/23/2022).
- [10] Lifewire. *Patch Tuesday: What It Is & Why You Should Care*. 2022. URL: <https://www.lifewire.com/patch-tuesday-2625783> (visited on 08/23/2022).
- [11] Christine Barrett. "New security features for Windows 11 will help protect hybrid work - Microsoft Security Blog". In: *Microsoft Security Blog* (2022). URL: <https://www.microsoft.com/security/blog/2022/04/05/new-security-features-for-windows-11-will-help-protect-hybrid-work> (visited on 08/23/2022).
- [12] Steve Morgan. *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*. 2021. URL: <https://cybersecurityventures.com/annual-cybercrime-report-2019> (visited on 08/23/2022).
- [13] Kacy Zurkus. "Orgs Slow to Advance IoT Security". In: *Infosecurity Magazine* (2019). URL: <https://www.infosecurity-magazine.com/news/orgs-slow-to-advance-iot-security> (visited on 08/23/2022).
- [14] Ashley Lukehart. *2021 Cyber Attack Statistics, Data, and Trends*. Ed. by Parachute Techs. Feb. 23, 2021. URL: <https://parachutetechs.com/2021-cyber-attack-statistics-data-and-trends/>.
- [15] Oxford English Dictionary. *internet, n*. Ed. by Oxford University Press. Sept. 18, 2022. URL: <https://www.oed.com/viewdictionaryentry/Entry/248411>.
- [16] Knud Lasse Lueth. *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time*. Tech. rep. IoT Analytics, Nov. 19, 2020. URL: <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time> (visited on 11/08/2022).
- [17] Richard Pinckney and Toby Headdon. "The value of data for the Internet of Things". In: *Lexology* (2022). URL: <https://www.lexology.com/library/detail.aspx?g=2019ca35-2e9b-433e-b296-a05a84ea4d98> (visited on 08/24/2022).

- [18] Keenan May. *How Embedded Sensors will Transform Workplace Performance, Employee Engagement, and Facility Management*. Tech. rep. CoWorkr, 2020. URL: <https://medium.com/coworkr/how-embedded-sensors-will-transform-workplace-performance-employee-engagement-and-facility-2a3fb9ae1142> (visited on 08/24/2022).
- [19] Elizabeth Dukes. “The Cost of IoT Sensors Is Dropping Fast”. In: *iOFFICE* (2022). URL: <https://www.iofficecorp.com/blog/cost-of-iot-sensors> (visited on 08/24/2022).
- [20] László Juhász. “Overview of industry 4.0 tools for cost-benefit analysis”. In: 4 (Oct. 2018), pp. 51–70.
- [21] Ogi Djuraskovic. *30+ Key Internet of Things (IoT) Statistics - 2022*. Ed. by FirstSiteGuide. Feb. 18, 2022. URL: <https://firstsiteguide.com/internet-of-things-stats> (visited on 08/24/2022).
- [22] Michael Shirer John Rydning. *Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts*. Tech. rep. International Data Corporation, Mar. 24, 2021. URL: <https://www.idc.com/getdoc.jsp?containerId=prUS47560321> (visited on 08/24/2022).
- [23] Tempo Automation. *Software-Accelerated Electronics Manufacturing Tempo Automation*. 2022. URL: <https://www.tempoautomation.com> (visited on 08/24/2022).
- [24] Zhanna Malekos Smith and Eugenia Lostri. *The Hidden Costs of Cybercrime*. Tech. rep. Center for Strategic & International Studies, Dec. 9, 2020. URL: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>.
- [25] Eli Amir, Shai Levi, and Tsafir Livne. “Do firms underreport information on cyber-attacks? Evidence from capital markets”. In: *Review of Accounting Studies* 23.3 (June 19, 2018), pp. 1177–1206. ISSN: 1573-7136. DOI: 10.1007/s11142-018-9452-4. (Visited on 08/24/2022).
- [26] Department for Digital, Culture, Media and Sport. *Cyber Security Breaches Survey 2017*. 2017. URL: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017> (visited on 08/24/2022).
- [27] ISACA. *New Study Reveals Cybercrime May Be Widely Underreported Even When Laws Mandate Disclosure*. June 3, 2019. URL: <https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/new-study-reveals-cybercrime-may-be-widely-underreported-even-when-laws-mandate-disclosure> (visited on 08/24/2022).
- [28] ENISA. *Botnets: Measurement, Detection, Disinfection and Defence*. Tech. rep. ENISA, Mar. 7, 2011. URL: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>.
- [29] Jens von Bergmann. *Public Health vs Scientists*. Mar. 17, 2021. URL: [https://github.com/mountainMath/xkcd\\_exponential](https://github.com/mountainMath/xkcd_exponential).
- [30] Oxford English Dictionary. *exponential, adj. and n.* Ed. by Oxford University Press. Sept. 18, 2022. URL: <https://www.oed.com/viewdictionaryentry/Entry/66689>.
- [31] Alexander Podkul et al. “The coronavirus exponential: A preliminary investigation into the public’s understanding”. In: *Harvard Data Science Review* 10 (May 14, 2020).
- [32] Vladimir Kuskov. *Honeypots and the Internet of Things*. Tech. rep. Kaspersky Labs, June 19, 2017. URL: <https://securelist.com/honeypots-and-the-internet-of-things/78751> (visited on 09/18/2022).
- [33] Mikhail Kuzin. *New trends in the world of IoT threats*. Tech. rep. Kaspersky Labs, Sept. 18, 2018. URL: <https://securelist.com/new-trends-in-the-world-of-iot-threats/87991> (visited on 09/18/2022).
- [34] Radware. *A Quick History of IoT Botnets - Radware Blog*. Ed. by Radware. Mar. 1, 2018. URL: <https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets> (visited on 09/18/2022).

- [35] Ben Dickson. *Why IoT Security Is So Critical*. Ed. by Techcrunch. Oct. 25, 2015. URL: <https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/>.
- [36] Irfan Saif. *Cyber risk in an Internet of Things world. Flashpoint edition 4: More data, more opportunity, more risk*. Ed. by deloitte. Oct. 29, 2015. URL: <https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html>.
- [37] Francisco Maroto. *5 Security Vulnerabilities Looming for the Internet of Things*. Ed. by DataFloq. June 24, 2016. URL: <https://datafloq.com/read/5-Security-Vulnerabilities-Looming-Internet-Things/2137>.
- [38] OWASP. *Internet of Things Top Ten*. Research rep. OWASP, 2014. URL: [https://owasp.org/www-pdf-archive/Internet\\_of\\_Things\\_Top\\_Ten\\_2014-OWASP.pdf](https://owasp.org/www-pdf-archive/Internet_of_Things_Top_Ten_2014-OWASP.pdf).
- [39] Internet of Things Security Foundation. *ESTABLISHING PRINCIPLES FOR INTERNET OF THINGS SECURITY*. Research rep. Internet of Things Security Foundation, Sept. 2015. URL: <https://www.iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf>.
- [40] Phil Muncaster. *EU Security Agency Enisa Set for IoT Role in 2016*. Ed. by infosecurity-magazine. Oct. 27, 2015. URL: <https://www.infosecurity-magazine.com/news/eu-security-agency-enisa-set-for/>.
- [41] ENISA. *ENISA Work programme for 2016 adopted: Agency builds on successful activities and broadens scope in 'smart' studies and IoT security*. Ed. by ENISA. Oct. 26, 2015. URL: <https://www.enisa.europa.eu/news/enisa-news/enisa-work-programme-for-2016-adopted-agency-builds-on-successful-activities-and-broadens-scope-in-2018smart2019-studies-and-iot-security>.
- [42] Check Point Research. *2017 Global Cyber Attack Trends Report*. Research rep. Check Point Software Technologies LTD, Jan. 31, 2018. URL: [https://www.checkpoint.com/downloads/product-related/infographic/H2\\_2017\\_Global\\_Cyber\\_Attack\\_Trends\\_Report.pdf](https://www.checkpoint.com/downloads/product-related/infographic/H2_2017_Global_Cyber_Attack_Trends_Report.pdf).
- [43] Melissa Michael. *Attack Landscape H1 2019: IoT, SMB traffic abound*. Ed. by f-secure. 2019. URL: <https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/>.
- [44] PYMNTS. *Kaspersky Detects 1.5B IoT Cyberattacks This Year*. Sept. 3, 2021. URL: <https://www.pymnts.com/news/security-and-risk/2021/kaspersky-detects-iot-cyberattacks-double-last-year/>.
- [45] James Stannard et al. *Consumer Attitudes Towards IoT Security*. Research rep. Ipsos MORI, 2020. URL: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/978685/Consumer\\_Attitudes\\_Towards\\_IoT\\_Security\\_-\\_Research\\_Report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf).
- [46] Vivienne Clarke. *Brexit 'will not impact' UK-EU co-operation on cybersecurity*. Ed. by The Irish Times. 2018. URL: <https://www.irishtimes.com/business/technology/brexit-will-not-impact-uk-eu-co-operation-on-cybersecurity-1.3682697>.
- [47] Julian Kings and John Scarlett. *The Future of UK-EU Security Cooperation*. Ed. by Royal United Services Institute (RUSI). Jan. 18, 2021. URL: <https://rusi.org/explore-our-research/publications/commentary/future-uk-eu-security-cooperation>.
- [48] Julian King. *Cybersecurity after Brexit*. Ed. by UK in a changing Europe. 2020. URL: <https://ukandeu.ac.uk/cybersecurity-after-brexit/>.
- [49] Tim Stevens. *UK Cybersecurity and Brexit*. Ed. by UK in a changing Europe. 2019. URL: <https://ukandeu.ac.uk/uk-cybersecurity-and-brexit/>.
- [50] Department for Digital, Culture, Media and Sport. *Proposal on ENISA and cyber security certification*. Dec. 20, 2017. URL: <https://www.gov.uk/government/consultations/proposal-on-enisa-and-cyber-security-certification>.

- [51] Department for Digital, Culture, Media and Sport. “Secure by Design report”. In: *GOV* (Mar. 7, 2018). URL: <https://www.gov.uk/government/publications/secure-by-design-report>.
- [52] Sam Trendall. “Government cybersecurity strategy lacks clear objectives, MPs say”. In: (June 6, 2019). Ed. by Civil Service World. URL: <https://www.civilserviceworld.com/professions/article/government-cybersecurity-strategy-lacks-clear-objectives-mps-say>.
- [53] Department for Digital, Culture, Media and Sport. “Code of Practice for Consumer IoT Security”. In: *GOV* (Oct. 14, 2018). URL: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>.
- [54] PETRAS IoT Hub. “Summary literature review of industry recommendations and international developments on IoT security”. In: *GOV* (Mar. 7, 2018). Ed. by Media Department for Digital Culture and Sport. URL: <https://www.gov.uk/government/publications/summary-literature-review-on-iot-security>.
- [55] ETSI. *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI EN 303 645 V2.1.1 (2020-06)*. V2.1.1. June 2020. URL: [https://www.etsi.org/deliver/etsi\\_en/303600\\_303699/303645/02.01.01\\_60/en\\_303645v020101p.pdf](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf).
- [56] European Telecommunications Standards Institute (ETSI). *ETSI Drafting Rules (EDR). Version adopted by the Director-General (29 March 2021)*. Mar. 29, 2021. Chap. 3.2. URL: [https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/43\\_ETSI\\_directives\\_20\\_may\\_2021\\_part2%20\(EDR\).pdf](https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/43_ETSI_directives_20_may_2021_part2%20(EDR).pdf).
- [57] ETSI. *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI TS 103 645 V1.1.1 (2019-02)*. V1.1.1. Feb. 2019. URL: [https://www.etsi.org/deliver/etsi\\_ts/103600\\_103699/103645/01.01.01\\_60/ts\\_103645v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf).
- [58] Harris Interactive. *Consumer Internet of Things Security Labelling Survey Research Findings*. Tech. rep. Harris Interactive, 2019. URL: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/950429/Harris\\_Interactive\\_Consumer\\_IoT\\_Security\\_Labelling\\_Survey\\_Report\\_V2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf).
- [59] Department for Digital, Culture, Media and Sport. “Government response to the Secure by Design informal consultation”. In: *GOV* (Oct. 14, 2018). URL: <https://www.gov.uk/government/publications/government-response-to-the-secure-by-design-informal-consultation/government-response-to-the-secure-by-design-informal-consultation>.
- [60] Department for Digital, Culture, Media and Sport. “Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation”. In: (Feb. 3, 2020). URL: <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation>.
- [61] Department for Digital, Culture, Media and Sport. “New cyber security laws to protect smart devices amid pandemic sales surge”. In: *GOV* (Apr. 21, 2021). URL: <https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge>.
- [62] ENISA. *Baseline Security Recommendations for IoT*. Tech. rep. ENISA, Nov. 20, 2017. URL: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>.
- [63] ENISA. *Guidelines for Securing the Internet of Things*. Tech. rep. ENISA, Nov. 9, 2020. URL: <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>.
- [64] ENISA. *Good Practices for Security of IoT. Secure Software Development Lifecycle Secure Software Development Lifecycle*. Tech. rep. ENISA, Nov. 19, 2019. URL: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>.

- [65] European Commission. *EU Cybersecurity plan to protect open internet and online freedom and opportunity*. Feb. 7, 2013.
- [66] European Parliament and of the Council of 6 July 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. cybersecurity of network and information systems*. July 6, 2016. URL: <http://data.europa.eu/eli/dir/2016/1148/oj>.
- [67] ENISA. *NIS Directive*. Ed. by ENISA. Nov. 29, 2018. URL: <https://www.enisa.europa.eu/topics/nis-directive?tab=details>.
- [68] European Commission. “The Cybersecurity Act strengthens Europe’s cybersecurity”. In: (Mar. 19, 2019). URL: <https://digital-strategy.ec.europa.eu/en/news/cybersecurity-act-strengthens-europes-cybersecurity>.
- [69] Luca Bertuzzi. “EU chief announces cybersecurity law for connected devices”. In: (Sept. 22, 2021). URL: <https://www.euractiv.com/section/cybersecurity/news/eu-chief-announces-cybersecurity-law-for-connected-devices>.
- [70] John M. Blythe, Nissy Sombatruang, and Shane D. Johnson. “What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?” In: *Journal of Cybersecurity* 5.1 (June 15, 2019). ISSN: 2057-2085. DOI: 10.1093/cybsec/tyz005.
- [71] National Cyber Security Center. *Cyber Aware*. 2023. URL: <https://www.ncsc.gov.uk/cyberaware/home> (visited on 08/23/2023).
- [72] John M. Blythe and Shane D. Johnson. *Rapid evidence assessment on labelling schemes and implications for consumer IoT security*. Research rep. Dawes Centre for Future Crime at UCL, Oct. 14, 2018. URL: <https://www.gov.uk/government/publications/rapid-evidence-assessment-on-labelling-schemes-for-iot-security>.
- [73] Signe Waechter, Bernadette Sütterlin, and Michael Siegrist. “Desired and Undesired Effects of Energy Labels: An Eye-Tracking Study”. In: *PLOS ONE* 10.7 (July 31, 2015). Ed. by Joseph Najbauer. DOI: 10.1371/journal.pone.0134132. URL: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0134132>.
- [74] Pardis Emami-Naeini et al. “Ask the Experts: What Should Be on an IoT Privacy and Security Label?” In: *2020 IEEE Symposium on Security and Privacy (SP)*. Feb. 2020, pp. 447–464. DOI: 10.1109/SP40000.2020.00043.
- [75] Michael McWhertor. *ESRB game ratings will now include loot box warnings, other ‘random item’ purchases*. Ed. by Polygon. Apr. 13, 2020. URL: <https://www.polygon.com/2020/4/13/21219071/esrb-game-ratings-loot-boxes-gacha-random-items>.
- [76] Office of National Statistics. *Internet access - households and individuals*. Aug. 7, 2020. URL: <https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/datasets/internetaccesshouseholdsandindividuals95confidenceintervals>.
- [77] GOV.UK. *Assisted digital support: an introduction*. Aug. 30, 2018. URL: <https://www.gov.uk/service-manual/helping-people-to-use-your-service/assisted-digital-support-introduction>.
- [78] GOV.UK. *Designing assisted digital support*. Aug. 30, 2018. URL: <https://www.gov.uk/service-manual/helping-people-to-use-your-service/designing-assisted-digital>.
- [79] GOV.UK. *Understanding users who don’t use digital services*. Aug. 30, 2018. URL: <https://www.gov.uk/service-manual/user-research/understanding-users-who-dont-use-digital-services>.
- [80] National Cyber Security Center. *Password Policy - Advice for system owners*. Nov. 19, 2018. URL: <https://www.ncsc.gov.uk/collection/passwords>.
- [81] Paul A. Grassi et al. *NIST Special Publication 800-63B*. Tech. rep. NIST, June 2017. URL: <https://pages.nist.gov/800-63-3/sp800-63b.html#sec5>.

- [82] Global System for Mobile Communications. *GSMA Coordinated Vulnerability Disclosure Programme*. 2019. URL: <https://webcache.googleusercontent.com/search?q=cache:ztgZWjVnM5cJ:https://www.gsma.com/aboutus/workinggroups/fraud-security-group/gsma-coordinated-vulnerability-disclosure-programme+&cd=3&hl=en&ct=clnk&gl=uk>.
- [83] International Organization for Standardization. “ISO/IEC 29147:2018 (Vulnerability disclosure)”. In: *International Organization for Standardization* (Oct. 2018). URL: <https://www.iso.org/standard/72311.html>.
- [84] notarealhacker. *I reported a critical vulnerability in the KYC website of Sentinel Chain ICO and now they started a police investigation against me*. 2018. URL: <http://archive.is/j2Ucu>.
- [85] Pascal Meunier. “Reporting Vulnerabilities is for the Brave”. May 22, 2006. URL: <http://www.cerias.purdue.edu/site/blog/post/reporting-vulnerabilities-is-for-the-brave>.
- [86] Autorita’ Garante della Concorrenza e. del Mercato. *Apple and Samsung fined for software updates that have caused serious troubles and/or have reduced functionality of some mobile phones*. Oct. 24, 2018. URL: <https://en.agcm.it/en/media/press-releases/2018/10/PS11009-PS11039>.
- [87] Advanced Micro Devices, Inc. *Radeon RX on Twitter*. Nov. 29, 2015. URL: <https://twitter.com/Radeon/status/671058196547706880>.
- [88] Ian Paul. “AMD pushes Crimson driver fan speed hotfix after reports of overheating Radeon cards”. In: *PCWorld* (Dec. 1, 2015). Ed. by PC World. URL: <https://www.pcworld.com/article/418557/amd-pushing-crimson-driver-fan-speed-hotfix-after-reports-of-overheating-radeon-cards.html>.
- [89] John Steven, Jim Manico, and Dominique Righetto. “OWASP Password\_Storage\_Cheat\_Sheet”. May 9, 2019. URL: [https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Password\\_Storage\\_Cheat\\_Sheet.md](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Password_Storage_Cheat_Sheet.md).
- [90] Christopher Domas. “PROJECT ROSENBRIDGE - Hardware Backdoors in x86 CPUs”. July 27, 2018. URL: <https://i.blackhat.com/us-18/Thu-August-9/us-18-Domas-God-Mode-Unlocked-Hardware-Backdoors-In-x86-CPUs-wp.pdf>.
- [91] National Cyber Security Center. *Using TLS to protect data*. Nov. 19, 2018. URL: <https://www.ncsc.gov.uk/guidance/tls-external-facing-services>.
- [92] Razieh Hedayati and Seyedakbar Mostafavi. “A Lightweight Image Encryption Algorithm for Secure Communications in Multimedia Internet of Things”. In: *Wireless Personal Communications* (Oct. 2, 2021). ISSN: 1572-834X. DOI: 10.1007/s11277-021-09173-w.
- [93] Sergio García Gil. *Characteristics and evaluation of IEEE 802.11n standard*. Research rep. Castelldefels School of Telecommunications and Aerospace Engineering, July 16, 2013. URL: <https://core.ac.uk/download/pdf/41810065.pdf>.
- [94] Wi-Fi Alliance. *Wi-Fi CERTIFIED 6. Capacity, efficiency, and performance for advanced connectivity*. 2021. URL: <https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6>.
- [95] Laurent Simon and Ross Anderson. “Security Analysis of Android Factory Resets”. Research rep. University of Cambridge, 2015. URL: [https://www.cl.cam.ac.uk/~rja14/Papers/fr\\_most15.pdf](https://www.cl.cam.ac.uk/~rja14/Papers/fr_most15.pdf).
- [96] Amazon.com, Inc. *Set Up Your Dash Button Device*. Apr. 5, 2019. URL: <https://web.archive.org/web/20190405160830/https://www.amazon.com/gp/help/customer/display.html?nodeId=201746340>.
- [97] Amazon.com, Inc. *Vulnerability Reporting - Amazon Web Services (AWS)*. 2019. URL: <https://aws.amazon.com/security/vulnerability-reporting>.
- [98] Amazon.com, Inc. *Deactivated Amazon Dash Devices*. 2019. URL: <https://www.amazon.com/gp/help/customer/display.html?nodeId=201746340>.
- [99] Amazon.com, Inc. *Amazon.com Help: Set Up Your Echo*. 2019. URL: <https://www.amazon.com/gp/help/customer/display.html?nodeId=201601770>.
- [100] Amazon.com, Inc. *Amazon.com Help: Alexa Device Software Updates*. 2019. URL: <https://www.amazon.com/gp/help/customer/display.html?nodeId=201602210>.

- [101] Amazon.com, Inc. *Fire OS 8 for Fire Tablets*. May 17, 2022. URL: <https://developer.amazon.com/docs/fire-tablets/fire-os-8.html>.
- [102] Amazon.com, Inc. *Amazon.com Help: Set Up Your Echo Device with a Screen*. 2019. URL: <https://www.amazon.com/gp/help/customer/display.html?nodeId=G3BQ3JBVCELFGBEM>.
- [103] August Home, Inc. *How to Install: Doorbell Cam, 1st Gen*. 2022. URL: <https://support.august.com/doorbell-cam-installation-guide-introduction-r1VegvLyAdf>.
- [104] ASSA ABLOY. “Responsible Disclosure Policy”. In: (2022). URL: <https://www.assaabloy.com/group/en/about-us/product-security/disclosure-policy> (visited on 08/30/2022).
- [105] August Home, Inc. *How is Lock Firmware Updated?* 2022. URL: [https://support.august.com/updating-lock-firmware-SkGyPU1R\\_f](https://support.august.com/updating-lock-firmware-SkGyPU1R_f).
- [106] August Home, Inc. *August Smart Lock Install Guide*. 2014. URL: <http://in-app-installation-guides.s3-website-us-west-2.amazonaws.com/prod/installation/pdf/August-Smart-Lock-Install-Guide.pdf>.
- [107] Richard Clark. *Sphero BB8 robot toy The Missing Manual*. Dec. 24, 2015. URL: <https://medium.com/@phirate/sphero-bb8-robot-toy-the-missing-manual-5f275f1fae98>.
- [108] Sphero, Inc. *Vulnerability Disclosure Program*. 2018. URL: <https://support.sphero.com/article/5drs94lhk5-vulnerability-disclosure-program>.
- [109] Sphero, Inc. *Sphero Firmware Updates*. Ed. by Mike Moran. 2018. URL: <https://support.sphero.com/article/fnq9npsogu-sphero-firmware-updates>.
- [110] Belkin International, Inc. *Wemo Setup*. 2020. URL: <https://www.belkin.com/uk/support-article?articleNum=8218>.
- [111] Belkin International, Inc. *COORDINATED VULNERABILITY DISCLOSURE PROGRAM*. 2019. URL: <https://www.belkin.com/us/security>.
- [112] Belkin International, Inc. *Belkin Official Support - How to resolve Wemo firmware update error*. 2019. URL: <https://www.belkin.com/us/support-article?articleNum=8297>.
- [113] Belkin International, Inc. *Linksys Official Support - Linksys End of Life (Obsolete Products) Part 3*. 2019. URL: <https://www.linksys.com/us/support-article?articleNum=291978>.
- [114] Belkin International, Inc. *Belkin Official Support - Setting up the Wemo Smart Light Switch, F7C030*. 2019. URL: <https://www.belkin.com/us/support-article?articleNum=8185>.
- [115] Bitdefender. *How to set up Bitdefender BOX*. 2021. URL: <https://www.bitdefender.com/consumer/support/answer/3320/>.
- [116] Bitdefender. *Bitdefender Bug Bounty Program*. 2019. URL: <https://www.bitdefender.com/site/view/bug-bounty.html>.
- [117] Bitdefender. “[Product Update] Your Bitdefender BOX can now protect against eavesdropping by digital assistants with a new feature called Private Mode”. In: (Sept. 11, 2019). URL: <https://www.bitdefender.com/blog/hotforsecurity/product-update-bitdefender-box-can-now-protect-eavesdropping-digital-assistants-new-feature-called-private-mode/>.
- [118] Bitdefender. “Bitdefender BOX v.1 will reach End of Life on July 1, 2021”. In: (June 1, 2021). URL: <https://www.bitdefender.com/consumer/support/answer/2469/>.
- [119] Control4. *Control4® System Quick Start Guide*. 2016. URL: <https://www.control4.com/docs/product/control4-system/quick-start-guide/latest/control4-system-quick-start-guide-rev-u.pdf>.
- [120] Control4. *OS 3 Control4*. 2019. URL: <https://www.control4.com/os3>.
- [121] Control4. *Composer HE Getting Started*. 2014. URL: <https://www.control4.com/docs/product/composer-he/getting-started/english/revision/M/composer-he-getting-started-rev-m.pdf>.



- [122] S. A. S. Plume Labs. *How do I install my Flow?* 2019. URL: <https://plumelabs.zendesk.com/hc/en-us/articles/360006045613-How-do-I-install-my-Flow->.
- [123] S. A. S. Plume Labs. *How do I update my Flow's firmware?* 2019. URL: <https://plumelabs.zendesk.com/hc/en-us/articles/360012139513-How-do-I-update-my-Flow-s-firmware->.
- [124] Airboxlab S.A.S. *Install & setup your Foobot.* 2019. URL: <https://help.foobot.io/hc/en-us/articles/204713582-Install-setup-your-Foobot>.
- [125] Airboxlab S.A.S. *Foobot's update.* 2019. URL: <https://help.foobot.io/hc/en-us/articles/204716572>.
- [126] Alphabet Inc. *Set up your Google Home speaker or Google Nest display - Android - Google Nest Help.* 2019. URL: <https://support.google.com/googlenest/answer/7029485>.
- [127] Alphabet Inc. *Google Vulnerability Reward Program (VRP) Rules.* 2019. URL: <https://www.google.com/about/appsecurity/reward-program>.
- [128] Alphabet Inc. *Google Home firmware versions - Google Nest Help.* 2019. URL: <https://support.google.com/googlenest/answer/7365257?hl=en>.
- [129] Alphabet Inc. *Auto Update policy - Google Chrome Enterprise Help.* 2019. URL: <https://support.google.com/chrome/a/answer/6220366>.
- [130] Linquet Technologies Inc. *Linquet Frequently Asked Questions.* 2019. URL: <https://linquet.com/faq>.
- [131] Logitech International. *Getting Started with Harmony Elite.* 2019. URL: <https://support.myharmony.com/en-gb/elite>.
- [132] Logitech International. *Security Vulnerability Reporting.* 2019. URL: <https://www.logitech.com/en-us/legal/security-vulnerability-reporting.html>.
- [133] Logitech International. *How to update your Harmony firmware.* 2019. URL: <https://support.myharmony.com/en-us/how-to-update-your-firmware>.
- [134] Chris Welch. *Logitech will brick its Harmony Link hub for all owners in March.* 2017. URL: <https://www.theverge.com/circuitbreaker/2017/11/8/16623076/logitech-harmony-link-discontinued-bricked>.
- [135] Logitech International. *POP HOME SWITCH - Starter Pack Setup Guide.* 2017. URL: <https://www.logitech.com/assets/64671/19/pop-home-switch.pdf>.
- [136] S Thangam. *Re: My Logitech Pop Bridge flashes white 3 times every few seconds.* Ed. by Logitech Support. Jan. 2022. URL: <https://support.logi.com/hc/en-gb/community/posts/4416854753687/comments/4416917549847>.
- [137] Alphabet Inc. *How to connect your camera to the Nest app and install it - Google Nest Help.* 2019. URL: <https://support.google.com/googlenest/answer/9293657?hl=en>.
- [138] Alphabet Inc. *How to keep your Nest products and the Nest app up to date - Google Nest Help.* 2019. URL: <https://support.google.com/googlenest/answer/9335964?hl=en>.
- [139] Alphabet Inc. *How to set up your Nest thermostat - Android - Google Nest Help.* 2019. URL: <https://support.google.com/googlenest/answer/9266423?hl=en-GB>.
- [140] Alphabet Inc. *How to install your Nest Protect - Google Nest Help.* 2019. URL: [https://support.google.com/googlenest/answer/9231672?hl=en-GB&ref\\_topic=9346895](https://support.google.com/googlenest/answer/9231672?hl=en-GB&ref_topic=9346895).
- [141] Netgear Inc. *How do I set up my Orbi router and satellite?* 2019. URL: <https://kb.netgear.com/31017/How-do-I-set-up-my-Orbi-router-and-satellite>.
- [142] Netgear Inc. *NETGEAR Product Security - Report Vulnerabilities.* 2019. URL: <https://www.netgear.com/about/security>.
- [143] Netgear Inc. *Orbi Tri-band WiFi System - Downloads.* 2019. URL: <https://www.netgear.com/support/product/orbi.aspx#download>.
- [144] Virtual Graffiti Inc. *NETGEAR End of Life Products.* 2019. URL: <https://www.netguardstore.com/Netgear-EOL.asp>.

- [145] Particle.io. *Flash Apps with Particle Build - Logging In*. 2019. URL: <https://docs.particle.io/tutorials/developer-tools/build/photom>.
- [146] Matthew Mcgowan et al. *particle-iot/device-os/CHANGELOG*. 2019. URL: <https://github.com/particle-iot/device-os/blob/release/stable/CHANGELOG.md>.
- [147] Particle.io. *Particle Product Lifecycle Policy*. 2019. URL: <https://docs.particle.io/support/general/product-lifecycle-policy>.
- [148] Craig Lloyd. *How to Set Up Your Philips Hue Lights*. 2017. URL: <https://www.howtogeek.com/247500/how-to-set-up-your-philips-hue-lights>.
- [149] Koninklijke Philips. *Philips Responsible Disclosure Statement*. 2019. URL: <https://www.philips.com/a-w/security/coordinated-vulnerability-disclosure.html>.
- [150] Koninklijke Philips. *End of Support Policy Philips Hue*. 2019. URL: <https://www2.meethue.com/en-us/support/end-of-support-policy>.
- [151] Koninklijke Philips. *hue Quick Start Guide*. 2017. URL: [https://images.philips.com/is/content/PhilipsConsumer/PDFDownloads/Global/Meethue/product-support/ODLI20170713-001-UPD-en\\_AA-hue-go-emea.pdf](https://images.philips.com/is/content/PhilipsConsumer/PDFDownloads/Global/Meethue/product-support/ODLI20170713-001-UPD-en_AA-hue-go-emea.pdf).
- [152] Amazon.com, Inc. *Setting Up Your Ring Video Doorbell in the Ring App*. 2019. URL: <https://support.ring.com/hc/en-gb/articles/115001773266>.
- [153] Amazon.com, Inc. *Updating the Firmware For Your Ring Devices*. 2019. URL: <https://support.ring.com/hc/en-us/articles/115004599926-Checking-and-Updating-Your-Firmware>.
- [154] Andrew. *Farewell TrackR*. Ed. by geeknewscentral. Sept. 22, 2021. URL: <https://geeknewscentral.com/2021/09/22/farewell-trackr/>.
- [155] Department for Digital, Culture, Media and Sport. “Pledges from industry to implement the Code of Practice for Consumer IoT Security”. In: *GOV* (Oct. 14, 2018). URL: <https://www.gov.uk/government/publications/pledges-from-industry-to-implement-iot-security-code-of-practice> (visited on 10/03/2022).
- [156] Verizon. *2022 Data Breach Investigations Report*. Tech. rep. Verizon Business, 2022. URL: <https://www.verizon.com/business/resources/reports/dbir> (visited on 10/03/2022).
- [157] Christopher Domas. *P R O J E C T : R O S E N B R I D G E Hardware Backdoors in x86 CPUs*. Tech. rep. Black Hat USA 2018, July 27, 2018. URL: <https://www.blackhat.com/us-18/briefings/schedule/#god-mode-unlocked---hardware-backdoors-in-x-cpus-10194> (visited on 10/03/2022).
- [158] Sam Bowne. *Amazon Password Vulnerabilities*. July 3, 2018. URL: <https://samsclass.info/129S/proj/amp.htm> (visited on 09/26/2022).
- [159] YesWeHack. *FireBounty Amazon Vulnerability Research Program Vulnerability Disclosure Program*. Apr. 24, 2020. URL: <https://firebounty.com/2872-amazon-vulnerability-research-program> (visited on 09/26/2022).
- [160] August Home, Inc. *Setting Up Your Doorbell Camera in the August App*. 2021. URL: <https://support.august.com/setting-up-your-doorbell-cam-pro-rlxwLkRdf>.
- [161] Michael Schneider and Veit Hailperin. *Belkin WeMo Switch Communications Analysis*. Tech. rep. scip, Feb. 18, 2016. URL: <https://www.scip.ch/en/?labs.20160218> (visited on 09/26/2022).
- [162] Alphabet Inc. *Add your Nest thermostat to the Nest app*. 2022. URL: <https://support.google.com/googlenest/answer/9301088?hl=en-GB#section-4&zippy=,create-an-account-in-the-nest-app>.
- [163] Alphabet Inc. *Check for an account that exists - Google Account Help*. 2022. URL: <https://support.google.com/accounts/answer/40560?hl=en> (visited on 09/26/2022).
- [164] Bugcrowd. *Standard Disclosure Terms - Bugcrowd*. 2022. URL: <https://www.bugcrowd.com/resources/essentials/standard-disclosure-terms> (visited on 09/26/2022).

- [165] Make It Clear. *DCMS - Internet of Things (IoT) labelling online study*. Ed. by Rick Harrison. July 2020. URL: <https://makeitclear.com/insight/dcms-internet-of-things-iot-labelling-online-study>.
- [166] Organisation for Economic Co-operation and Development. “Promoting sustainable consumption: good practices in OECD countries”. In: *Organisation for Economic Co-operation and Development (OECD)* (May 2008). URL: <https://apo.org.au/node/1515>.
- [167] World Health Organisation. *Global Strategy on Diet, Physical Activity and Health - 2004*. Mar. 2004. URL: <https://www.who.int/publications/i/item/9241592222>.
- [168] Manon Egnell et al. “Objective Understanding of Front-of-Package Nutrition Labels: An International Comparative Experimental Study across 12 Countries”. In: *Nutrients* 10.10 (Oct. 2018), p. 1542. ISSN: 2072-6643. DOI: 10.3390/nu10101542.
- [169] Ellen Van Kleef and Hans Dagevos. “The Growing Role of Front-of-Pack Nutrition Profile Labeling: A Consumer Perspective on Key Issues and Controversies”. In: *Critical Reviews in Food Science and Nutrition* 55.3 (2013), pp. 291–303. DOI: 10.1080/10408398.2011.653018. eprint: <https://doi.org/10.1080/10408398.2011.653018>. URL: <https://doi.org/10.1080/10408398.2011.653018>.
- [170] European Commission. *In focus: A new generation of EU energy labels*. Aug. 2020. URL: [https://ec.europa.eu/info/news/focus-new-generation-eu-energy-labels-2020-aug-13\\_en](https://ec.europa.eu/info/news/focus-new-generation-eu-energy-labels-2020-aug-13_en).
- [171] Patrick Gage Kelley et al. “Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '10. Atlanta, Georgia, USA: Association for Computing Machinery, 2010, pp. 1573–1582. ISBN: 9781605589299. DOI: 10.1145/1753326.1753561. URL: <https://doi.org/10.1145/1753326.1753561>.
- [172] Shih-Chung Lee. “Perceptual Considerations in Icon Design for Instructional Communication on JSTOR”. In: *Educational Technology* 36.2 (1996), pp. 58–60. URL: <https://www.jstor.org/stable/44428330> (visited on 11/08/2022).
- [173] UX Pickle. *Why Is UX so Difficult? - UX Pickle*. Sept. 26, 2021. URL: <https://uxpickle.com/why-is-ux-so-difficult> (visited on 11/08/2022).
- [174] Aurora Harley. *Icon Usability*. Ed. by Nielsen Norman Group. July 27, 2014. URL: <https://www.nngroup.com/articles/icon-usability> (visited on 12/05/2022).
- [175] Ben Shneiderman et al. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. 6th. Pearson, Apr. 30, 2016. ISBN: 013438038X.
- [176] Robin L. Kelly. *H.R.1668 - 116th Congress (2019-2020): IoT Cybersecurity Improvement Act of 2020*. Mar. 11, 2019. URL: <https://www.congress.gov/bill/116th-congress/house-bill/1668> (visited on 10/02/2022).
- [177] Michael Fagan et al. “Profile of the IoT Core Baseline for Consumer IoT Products”. In: *CSRC | NIST* (Sept. 2022). DOI: 10.6028/NIST.IR.8425. (Visited on 10/02/2022).
- [178] Australian Government. *Voluntary Code of Practice*. Sept. 3, 2020. URL: <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice> (visited on 10/02/2022).
- [179] Infocomm Media Development Authority. *IMDA Launches IoT Cyber Security Guide to Help Enterprise Users and Vendors Secure IoT Systems - Infocomm Media Development Authority*. Mar. 13, 2020. URL: <https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/IMDA-Launches-IoT-Cyber-Security-Guide-to-Help-Enterprise-Users-and-Vendors-Secure-IoT-Systems> (visited on 10/02/2022).
- [180] Megan L. Head et al. “The Extent and Consequences of P-Hacking in Science”. In: *PLoS Biology* 13.3 (Mar. 13, 2015). DOI: 10.1371/journal.pbio.1002106. (Visited on 10/11/2022).
- [181] PDFlib. *PDFlib: The PDF/A Standards*. Sept. 6, 2022. URL: <https://www.pdfliib.com/pdf-knowledge-base/pdfa/the-pdfa-standards> (visited on 09/06/2022).

[182] International Organization for Standardization. *ISO 19005-3:2012*. Tech. rep. 2012. URL: <https://www.iso.org/standard/57229.html> (visited on 09/06/2022).

all

## Part VI

# Appendices

## 15 Survey Files

For user studies, the following were provided. These are three documents, expressed each in three formats for increased accessibility. If your PDF reader does not support embedded files (a feature since PDF/A-3 in 2012 [181], ISO 19005-3:2012 [182]) you can extract these files from the document, sometimes download them separately from the page you are viewing this document as accompanying files, or upgrade to a PDF reader which supports PDF/A-3.

QuestionsParticipantVersion-2.docx

QuestionsParticipantVersion-2.odt

QuestionsParticipantVersion-2.pdf

template-participant-consent-form.docx

template-participant-consent-form.odt

template-participant-consent-form.pdf

template-participant-information-factsheet.docx

template-participant-information-factsheet.odt

template-participant-information-factsheet.pdf

Spreadsheet for Survey Results, including analysis of results

## 16 Focus Group Files

The following are the documents provided to participants in each focus group. If your PDF reader does not support embedded files (a feature since PDF/A-3 in 2012 [181], ISO 19005-3:2012 [182]) you can extract these files from the document, sometimes download them separately from the page you are viewing this document as accompanying files, or upgrade to a PDF reader which supports PDF/A-3.

FOCUSGROUPtemplate-participant-consent-form.docx

FOCUSGROUPtemplate-participant-consent-form.odt

FOCUSGROUPtemplate-participant-information-factsheet.docx

FOCUSGROUPtemplate-participant-information-factsheet.odt

FocusGroupPart1.docx

FocusGroupPart1.odt

The following are the automatic transcriptions of the discussions in each focus group. The transcriptions may not be entirely correct, but the original audio files cannot be shared (real names were used, and that would count as personally identifiable information, which was agreed to not be published)

AcademicFocusGroupAutoTranscript.docx

CyberProfessionalsFocusGroupAutoTranscript.docx

## 17 Raw Image Files

### 17.1 Survey Figures

 Figure 1

 Figure 2

Figure 3 is a duplicate of Figure 1


 Figure 4


 Figure 5

 Figure A

 Figure B

 Figure C

 Miniature Label

 Alternative Mini Label

### 17.2 Label Icons

Originals are followed by their “Squared” variants when available.

 Icon One  Icon One [Squared]

 Icon Two  Icon Two [Squared]

 Icon Three  Icon Three [Squared]

 Icon Four  Icon Four [Squared]

 Icon Five  Icon Five [Squared]

 Icon Six  Icon Six [Squared]

 Icon Seven  Icon Seven [Squared]

 Icon Eight  Icon Eight [Squared]

 Icon Nine  Icon Nine [Squared]

 Icon Ten  Icon Ten [Squared]









 Icon Eleven  Icon Eleven [Squared]

 Icon Twelve-One  Icon Twelve-One [Squared]

 Icon Twelve-Two  Icon Twelve-Two [Squared]




















 Icon Thirteen  Icon Thirteen [Squared]

 Icon Fourteen  Icon Fourteen [Squared]

-  Certified, with calendar  Certified, with calendar [Squared]
-  Certified, with date+tick  Certified, with date+tick [Squared]
-  Certified, with tick  Certified, with tick [Squared]
-  Inverted Certification Logo
-  Updates Until Logo

### **17.3 Fullsize Document Figures**

All document figures, attached instead of embedded, such that you can view them in stand-alone format.

-  Figure 11
-  Figure 25
-  Figure 5 Additionally, you may click this text for the Source Table of this Figure
-  Figure 4
-  Figure 12
-  Figure 14
-  Figure 13
-  Figure 2
-  Figure 3
-  Figure 1
-  Figure 23
-  Figure 15
-  Figure 16
-  Figure 17
-  Figure 18
-  Figure 19
-  Figure 20
-  Figure 21
-  Figure 22