Journal of Cybersecurity, 2019, 1–10
doi: 10.1093/cybsec/tyz005
Research paper

Research paper

What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?

John M. Blythe[1,2,*], Nissy Sombatruang[1] and Shane D. Johnson[1]

[1]Department of Security and Crime Science, University College London, 35 Tavistock Square, London WC1H 9EZ, UK
[2]CybSafe, Level 39, One Canada Square, Canary Wharf, London E14 5AB, UK

*Correspondence address: Department of Security and Crime Science, University College London, 35 Tavistock Square, London WC1H 9EZ, UK. Tel: +44 (0) 203 675 1903; E-mail: j.blythe@ucl.ac.uk

Received 4 February 2019; revised 2 May 2019; accepted 2 May 2019

Abstract

Through the enhanced connectivity of physical devices, the Internet of Things (IoT) brings improved efficiency to the lives of consumers when on-the-go and in the home. However, it also introduces new potential security threats and risks. These include threats that range from the direct hacking of devices that could undermine the security, privacy and safety of its users, to the enslaving of IoT devices to commit cybercrime at scale, such as Denial of Service attacks. The IoT is recognized as being widely insecure, in large part, due to the lack of security features built into devices. Additionally, consumers do not always actively use security features when available. More disconcerting is that we lack market surveillance on whether manufacturers ship products with good security features or how the importance of user-controlled security features is explained to IoT users. Our study seeks to address this gap. To do this, we compiled a database of 270 consumer IoT devices produced by 220 different manufacturers on sale at the time of the study. The user manuals and associated support pages for these devices were then analysed to provide a 'consumer eye' view of the security features they provide and the cyber hygiene advice that is communicated to users. The security features identified were then mapped to the UK Government's Secure by Design Code of Practice for IoT devices to examine the extent to which devices currently on the market appear to conform to it. Our findings suggest that manufacturers provide too little publicly available information about the security features of their devices, which makes market surveillance challenging and provides consumers with little information about the security of devices prior to their purchase. On average, there was discussion of around four security features, with account management and software updates being the most frequently mentioned. Advice to consumers on cyber hygiene was rarely provided. Finally, we found a lack of standardization in the communication of security-related information for IoT devices among our sample. We argue for government intervention in this space to provide assurances around device security, whether this is provided in a centralized or decentralized manner.

Key words: Internet of Things; IoT security; consumer IoT

Introduction

The next wave of technological revolution is hyped to be the Internet of Things (IoT). These 'things' are Internet-connected devices that collect and share data over the Internet. This increased connectivity can help to improve their functionality and efficiency but in doing so also generates new potential threats and risks. Some of these devices represent new products (e.g. personal assistants) but many were once everyday household items such as light bulbs, thermostats and door locks. To provide an example of the risks these devices bring, consider that traditionally, protecting one's home generally only required adequate physical security measures. However, with the Internet connectedness that the IoT affords, protecting one's home now involves a cyber element with risks that no longer rely on geographical location. Among other things, threats to this cyber element can allow offenders to circumvent the very conventional physical security measures that protect our homes—door locks, windows and so on. IoT products can also interact with the home environment in new and innovative ways, and actuators within the products can directly impact on critical services within the home, such as heating systems. The disruption to such services can thus impact on human life and well-being [1] and as such, the security of the IoT is paramount to protect consumer's privacy, security and now physical safety [2].

However, most consumer IoT devices that are sold on the market are not secure by design [3]. Manufacturers lack the capacity to support modern security controls and updates [4] and are not sufficiently focused on security and privacy as a design priority [5]. In reality, security is left to the end stages of product design and in some cases, left until the product is on the market [6]. This is an unintended consequence of the 'lean' and agile product development life cycle that businesses choose to adopt. This is perhaps not surprising as there is currently little (if any) economic incentive for manufacturers to address security and there exists no regulation [2]. Consequently, as security is not prioritized, we continue to see examples of how insecure IoT devices are. For example, a 2014 study by HP found that 7 of the 10 most popular devices contained vulnerabilities associated with encryption and password security [7]. An investigation by which found that 8 out of 15 tested devices, which included Wi-Fi routers, children's toys and CCTV cameras, had security vulnerabilities [8]. Through vulnerability testing, academic research has also demonstrated that a number of security issues are consistently found [9–13]. This is the case even for large manufacturers who have the competency and resources to design secure products [9]. Discerning the security of an IoT product and communicating it in an accessible way is thus key to ensuring that consumers can make informed decisions about the IoT products they buy.

Discerning the security of Information Communication Technology (ICT) products is difficult. Discerning the security of IoT products is even more difficult, as doing so involves an assessment of the security of the IoT device, its cloud services, its application programming interface (API), and mobile applications [14]. IoT devices also have differing capabilities [15], with some devices lacking memory and physical capacity for security. Consequently, the IoT is seen as widely insecure [2] and this is in a large part due to the lack of security features built into products [3]. Due to such vulnerabilities, we have already seen a number of cyberattacks that have successfully exploited consumer IoT devices. Default login credentials and a lack of security updates are just some of the poor features that have been exploited at scale [16]. In response to the growing threats, governments and industry security champions have started to try and push manufacturers and the market toward better security.

In March 2018, the UK government outlined what they consider good security for consumer IoT products [17]. Their secure by design Code of Practice (CoP) outlines 13 principles that manufacturers should follow. They have also mapped the CoP onto existing standards and IoT security recommendations [18] demonstrating that the CoP is a useful overarching framework for IoT security. The CoP outlines the following security features that should be provided:

1. no default passwords;
2. implement a vulnerability disclosure policy;
3. keep software updated;
4. securely store credentials and security-sensitive data;
5. communicate securely;
6. minimize exposed attack surfaces;
7. ensure software integrity;
8. ensure that personal data are protected;
9. make systems resilient to outages;
10. monitor system telemetry data;
11. make it easy for consumers to delete personal data;
12. make installation and maintenance of devices easy;
13. validate input data.

Alongside the Department for Digital, Culture, Media & Sport (DCMS) CoP, there exist numerous IoT security best practice guides for manufacturers to follow [19]. However, what is not currently understood is what proportion of IoT devices on the market disclose the security features they offer to consumers. At present, only the findings of tests by security researchers [3, 20], consumer groups [21], and academic researchers [12] provide an indication of the security posture of IoT devices and market engagement with security. While important, such information provides only a partial picture. In this study, our primary aim was to identify what security features are currently communicated about IoT devices and how they map onto the DCMS CoP. To do this, we focused on the information communicated by manufacturers in device manuals and associated web pages (e.g. support pages and user forums). We chose to focus on these communication mechanisms as (i) it allowed us to scrutinize publicly available information about IoT devices, (ii) it allowed us to understand the challenges consumers face when buying IoT devices—since security information is communicated to them through manuals and support pages,[1] (iii) it provides a cost-effective method to identify security features compared to testing IoT products in the lab and (iv) it allowed us to sample a broader range of products than has been considered in previous research, by examining the products sold by UK retailers and those listed on IoT online databases (e.g. iotlist.co).

Considering previous work that has examined the security of devices, the approach taken largely focuses on assessing security for key areas, such as the confidentiality of data, the integrity and authentication of the IoT's connection, access control and the availability of the device to connection requests, and the capability of the device to participate in reflective distributed denial of service (DDoS) attacks [9]. Other approaches focus on the presence of security features and the 'vulnerability surface' of a device, i.e. features such as its interfaces, processing attack surface and systematic architecture that objectively make the device less secure [22]. Adopting a similar approach to Jamieson [22], we focus on the presence or absence of security features as a way to derive the security posture of a device as communicated in manuals and support pages. This allowed us to examine the security of a device at a lower cost than vulnerability testing individual IoT devices that other approaches require. A caveat, of course, is that the absence of a discussion of particular security features in device publications does not mean that

[1] Information may also be communicated through apps and other means during the set-up phase of a device, but consumers will not usually be able to access this information prior to purchasing a device. Moreover, the manuals and associated materials will represent an important source of information for many consumers.

those features are not present, just that they are not discussed in the materials that accompany a device. In terms of objectively assessing the security, a device offers this is an important methodological point. However, from the perspective of the consumer who wants to select a secure device prior to purchase, or who wants to be reassured about the security a purchased device provides, these are just semantics, since most consumers will not be able to conduct the highly technical penetration tests required to assess the limits of a device's security. Thus, the approach we take here provides a 'consumer eye' view of the security currently offered by devices.

A further challenge associated with consumer IoT is scalability, which makes market surveillance difficult [23]. Consumer IoT is already ubiquitous, but if the hype of the IoT matches reality, the majority of consumer goods will be Internet connected in the future (up from 6.4 billion connected 'things' to 20.8 billion by 2020 [24]). In this context, it will not be feasible to require manufacturers to go through independent penetration testing by third parties to obtain certification for all aspects of security. Thus, while the monitoring of compliance is clearly needed—to ensure that consumers are protected—the mechanism for doing this remains unclear. One suggestion is for the creation of a centralized database that details the security features of devices and provides an ongoing assessment of their security posture [23]. Presently, no such database exists and it is likely to be many years before such a resource is available. The assessment of device manuals and support pages thus allowed us to assess the current state of play concerning the disclosure of security features. As well as providing a snapshot of how things are currently, the exercise is intended to inform future market surveillance efforts.

The second aim of our study was to examine the provision of cyber hygiene advice from manufacturers. That is, 'what information is provided by manufacturers to encourage consumers to protect their devices and reduce their risk of cybercrime'. Statistics consistently show that consumers do not always engage in actions to protect themselves from cybersecurity threats. For example, only 52% regularly download the latest software updates and only 32% follow the latest government password advice [25]. Moreover, it is well known that the majority of cybersecurity breaches involve a human element [26] and so encouraging cyber hygiene is key to helping protect consumers and their devices. In the case of the IoT, this is even more challenging than it is for other ICT, as a number of the behaviours expected of consumers are the result of poor design (such as hard-coded default passwords) [17] rather than the result of consumer non-compliance. Research [27] has also shown that there are up to 43 security behaviours that consumers may have to engage in to protect their IoT devices from purchase (e.g. 'researching a device's security before purchasing'), set-up (e.g. 'changing security and privacy settings') and maintenance (e.g. 'updating devices') to ultimate disposal (e.g. 'securely wiping devices before disposal'). The burden for protecting devices is thus currently on consumers and manufacturers need to reduce this through greater 'security by design'. However, it is important to understand how well the features are described to consumers in user documentation and what (if any) crime prevention messaging is used to persuade consumers to follow them.

To summarize, in this study, we coded a sample of consumer IoT devices manuals and product support pages to provide a picture of the security features and cyber hygiene advice provided for different Internet-connected devices. We seek to address the following three research questions:

RQ_1: What security features are communicated in consumer IoT device manuals and support pages?

RQ_2: How well do the identified security features map onto the DCMS Secure by Design CoP?

RQ_3: What cyber hygiene advice is communicated to consumers?

Methodology

We compiled a database of consumer IoT devices from the website iotlist.co, and by extracting the names of devices listed under the categories 'smart home' or 'Internet of Things' from the website of a major UK retailer (PC World). We removed duplicate records and similar devices from the same manufacturers (e.g. different versions of the same device), which resulted in a database of 423 individual devices. Of these, 153 were no longer sold or in development. The final database consisted of 270 devices produced by 220 different manufacturers. While not important to the current work, this attrition is worth noting as it provides a crude illustration of the fact that IoT products may disappear from the market relatively quickly, which may create problems in the future if legacy devices and systems are not updated to keep them secure.

Search strategy for manuals and associated support pages

To identify device security features, the first step was to identify if the device came with a user manual. To locate the device manuals, we used Google's search engine and the following terms:

'Device name' AND 'manual' or 'guide' or 'quick start'

In addition to searching for the device manuals, we searched for associated online material published by the manufacturer that might communicate details about the security of devices to consumers. Such materials included support pages, user forums or frequently asked questions pages. We developed our search strategy using terms found in the DCMS CoP, as follows:

'Device name' AND 'security' or 'encryption' or 'password' or 'updates' or 'vulnerability disclosure'

Coding strategy

Two researchers independently read all of the materials identified and coded them using a 'bottom-up' approach. That is, they did not restrict the security features coded to those outlined in the DCMS CoP but rather coded any mention of device security features (as the DCMS CoP may not account for all security features). From these initial codes, a final coding scheme was derived—based on recurring codes from the initial data set—using the principles of content analysis [28]. Together, the two researchers re-coded the security features to the final coding scheme and mapped this to the DCMS CoP. Any disagreements were resolved through discussion and refinement of the coding scheme.

Results

Types of products

Table 1 shows the types of products identified from the iotlist.co and UK retailer's website, and the number of manuals or associated materials identified for each. In total, details were available in manuals and online pages for 42 devices, on online web pages only for 62 devices and in manuals alone for 66 devices. In terms of the types of IoT devices covered, wearables were the most common ($n = 46$), followed by home security ($n = 35$) and assistants ($n = 22$). Below, we first discuss our findings in the aggregate (i.e. for all devices) and then provide detail for specific types of devices.

Frequency of security features

The mean number of security features discussed[2] in the materials analysed was 4.11 (SD = 1.86, min = 1, max = 9, and $n = 170$). Of the nine devices for which the most security features were discussed (at least eight features), seven were produced by large manufacturers,[3] suggesting that larger manufacturers may provide greater disclosure of the security features their devices ship with. These larger manufacturers produced only 24% of the devices sampled and so this finding cannot simply be explained by their domination of the devices coded (i.e. they did not produce 7/9 of devices examined). Considering the security features discussed, user accounts were the most common (76.5%), followed by software/firmware updates (62.4%) and factory resets (48.2%) (Table 2). However, updates and factory resets were rarely actually framed around the discussion of security and in the majority of cases, were instead discussed in relation to performance improvement.

DCMS secure by design CoP

Considering the DCMS CoP, we were able to derive information from manuals and related support pages for 5 of the 13 principles. They are discussed here in order of prevalence.

CoP 3 ‘keep software updated’

Updates were one of the most commonly referenced features (62.4%). However, in the majority of cases (90%), the information provided did not explicitly mention security. Instead, updates were usually discussed in the context of product functionality, with quotes such as those below being typical:

> Free feature enhancements and product improvements are occasionally made available through firmware updates. We recommend keeping your <product name> up to date.
>
> Your <product name> device receives software updates automatically over an active Internet connection. These updates usually improve performance and add new features.

For only 10% of the devices examined was security explicitly mentioned as being an aspect of the updates provided. Example quotes from manuals/support pages included the following:

> Keep your beacons updated to enjoy all the new features which we add on a regular basis. Each update also brings performance improvements and security tweaks so you'll always want to have the latest firmware installed for the best experience.
>
> Keeping your watch up to date enhances its performance, improves apps' features, and adds more security protection. If an update is available, you will be receive a system notification on your watch. However, you can manually check for software updates.

Table 1: Frequency of type of products sampled

Type of product	Number of products without any information	Number of products with information discussed in user manual or website	Total
Wearable	15	31	46
Home security	7	28	35
Assistant	10	12	22
Smart energy	7	11	18
Smart lighting	9	6	15
Smart TV	3	12	15
Smart home monitoring	3	12	15
Smart gadgets	5	7	12
Smart health	5	6	11
Smart garden	3	6	9
Light control	5	3	8
Smart kitchen	4	4	8
Smart speaker	2	5	7
Smart transport	5	2	7
Smart baby monitors	2	5	7
Pet-related	4	2	6
Tracker	2	4	6
Exercise	4	1	5
Media centre		5	5
Children's devices	1	4	5
Bluetooth pen	2	1	3
Smart plug	1	2	3
Headphones	1	1	2
Total	100	170	270

CoP 11 ‘make it easy for consumers to delete personal data’

48.2% of products described some form of factory reset that could be used to clear the data stored on the device. However, for only 2.4% of devices was specific advice given to consumers on how to give away or sell their product and the procedures they should undertake for wiping their personal information. For the majority of devices, the discussion about factory resets was in relation to improving the performance of the device, e.g.:

> In case something goes terribly wrong with your <product name>, you have the option to perform a factory reset. Note that, when you do this, all your data and settings will be wiped from your <product name>.

CoP 2 ‘implement a vulnerability disclosure policy’

The materials provided for 32.4% of products detailed a vulnerability disclosure policy. This information was normally published on the manufacturers' website.

CoP 5 ‘communicate securely’

Discussions about the security of data and its communication were discussed with reference to the following: Wi-Fi encryption (20.0%), the encryption of data transmitted over the Internet or other channels (16.5%), encryption at rest but not on the device (15.3%), the security of cloud services (5.3%), local communication

[2] There were a possible total of 15 attributes - the need to change default passwords was excluded from this list because advice to change them indicates that a device was shipped with a default password (which is an insecure practice).

[3] These were Apple, Fitbit, NEST (2), Panasonic, Phillips, and Samsung.

Table 2: Prevalence of security features and DCMS CoP[a]

Security feature	Description	DCMS CoP No.	Devices (%)
User account management	Information was provided about account management (e.g. password protection, password reset, etc.)	NA	76.5
Software and firmware updates	Whether the device offered updates	(3)	62.4
Factory reset	Factory reset was available	(11)	48.2
Vulnerability disclosure policy	Whether the manufacturer has a vulnerability disclosure policy in place	(2)	32.4
Wi-Fi encryption standards[b]	Encryption standards were discussed (e.g. WPA and WPA2)	(5)	20.0
Data encryption in motion	Discussion of the encryption methods used when data are in motion (e.g. TLS and HTTPS)	(5)	16.5
Product lock	The device could be locked to prevent unauthorized access	NA	17.1
Encryption at rest	How data (e.g. AES) were encrypted when at rest were discussed	(5)	15.3
Cyber hygiene advice	Advice was given to encourage cybersecurity behaviours	(12)	10.0
Privacy features	Additional features discussed that help to protect the privacy of the user's data (e.g. limiting sharing of location)	NA	10.0
Permission management	Owner could delegate or revoke permissions for use and access to data stored on devices	NA	7.6
Security of the cloud	There was discussion of the security of the cloud services that the product used	(5)	5.3
No default passwords	Devices are not shipped with default passwords and require credentials to login	(1)	78
Local communications encryption	Information was provided about how local communications were encrypted	(5)	4.7
Local data storage	Data were only stored on the device locally	(5)	2.9
2FA	User was encouraged to use 2FA to secure online accounts	NA	1.8

[a] The fractions are for those products for which there was either a manual, online support pages or both.

[b] A breakdown of compatible and recommended Wi-Fi encryption standard is in Tables 3 and 4.

NA, not applicable.

Table 3: Device encryption standards discussed in manuals

Compatible Wi-Fi encryption standard ($n = 34$)						
Encryption standard	WEP	WPA	WPA2	WAC	WPS	Not specified
Number of devices	22	27	29	1	2	2
%	69	84	91	3	6	6

encryption such as Bluetooth and Z-wave (4.7%) and local data storage on the device (2.9%).

With respect to the specific types of Wi-Fi encryption used, this varied across the 34 products for which it was discussed, but most devices were compatible with more than one standard and most used the more secure Wi-Fi protected access (WPA) or Wi-Fi protected access II (WPA2) standards (Table 3). Details of other encryption standards used for IoT devices included in this review are in the Appendix.

CoP 12 'make installation and maintenance of devices easy'

This element of the CoP makes reference to the need to provide 'guidance on how to securely set up their device'. We found that for 10.0% of the devices, consumers were provided with advice about how to secure their IoT products.

CoP 1 'no default passwords'

According to the user manuals and associated materials, only 4.7% of the products sampled were shipped with a default password. Of the remainder, 77.6% required the user to create login credentials or a pin set-up instead of using default passwords. This suggests that this insecure practice of having default passwords may currently be in the minority.

Remaining CoP principles

From the information communicated to consumers, it was not possible to discern the extent to which the following CoP principles were addressed: CoP 4 'securely store credentials and security-sensitive data' CoP 6 'minimize exposed attack surfaces', CoP 7 'ensure software integrity', CoP 8 'ensure that personal data are protected', CoP 9 'make systems resilient to outages', CoP 10 'make systems resilient to outages' and CoP 13 'validate input data'.

Cyber hygiene and crime prevention advice

As discussed, our third overarching question concerned what advice is given to consumers about cyber security. We found that for 10.0% of products, some kind of advice was provided. The majority of the advice provided concerned password hygiene and how to create a 'strong password' (3.5%), although none of the advice was in line with the UK National Cyber Security Centre guidance on password creation. Instead, consumers were encouraged to create short and complex passwords (random letters, numbers and symbols). For example:

> . . . account password is secure enough to restrict access to your account. It should be at least eight-character long, have mixed case, and use a combination of alphanumeric and special characters.

The written materials provided for two products encouraged consumers to write their password down in the manual. For our sample, the material associated with only 34 devices (or 20% of the 170 devices) provided consumers with information about Wi-Fi security. Of these, the majority did not provide specific recommendations about the encryption standard consumers should use. Table 4 shows the number of devices for which Wi-Fi encryption was

Table 4: Wi-Fi encryption standards recommended to consumers

Recommended Wi-Fi encryption standard to users ($n = 34$)[a]

Recommended encryption standard	No recommendation	WPA	WPA2	WPA/WPA2
Number of devices	23	0	4	2
%	69	0	9	6

[a]Five devices used only one Wi-Fi encryption standard or did not specify which standards were used, and so for these, there was no recommendation.

discussed, and where more than one standard was provided, which was the preferred option.

For less than 2% (1.2%) of products, there was a discussion of the need for consumers to install updates for security reasons, despite software updates being discussed as a feature for 62.4% of products. The materials reviewed for two products provided general guidance on how consumers could protect themselves and their home in reference to cybercrime. For example:

> Q: How can I prevent a cybercriminal from making unauthorized changes to my thermostat?
>
> A: If a cybercriminal gains access to your Wi-Fi router, they can tamper with a wide range of online activities, including the settings on your connected devices. Make sure you change the default password on your Wi-Fi router, and when you select a new password, make sure it uses multiple upper- and lower-case letters and special characters.

Finally, 2.4% provided guidance on how to give away or sell a product whilst keeping data safe. For example:

> For security purposes, if you give away or recycle your <product name>, make sure you first remove any personal data. To erase your . . ..

None of the communications around cyber hygiene advice communicated the risks of non-compliance to the consumer.

Type of product

Table 5 provides a breakdown of the security features discussed in user manuals and associated materials by type of product. When looking at this, it is important to note that the sample size differs by product. And, while we sampled devices listed on a major retailer's website and Iotlist.co, our list of devices is not exhaustive and it is possible that our sample is not representative of the population of devices in use today. As such, we suggest that the data are interpreted cautiously. However, there are a number of trends worth noting. First, for our sample, home entry and smart health devices appeared to provide more cyber hygiene advice in their manuals than was the case for other products. Secondly, and somewhat expected, devices with a direct interface on the product were more likely to provide a product lock function (e.g. smart TVs). Thirdly, smart entry products had the highest frequency of permission settings. Finally, the bad practice of shipping with default passwords or Pins was highest for smart TVs.

Discussion

The current study aimed to (i) identify what security features are communicated to consumers in device manuals and support pages, (ii) explore the extent to which these features can be mapped onto the DCMS Secure by Design CoP and (iii) identify what cyber hygiene advice is communicated to consumers. Our review suggests that manufacturers are not providing enough information to consumers about the security features of their devices. On average, there was discussion of around four security features, with account management and software updates being the most frequently mentioned. Despite these features being important for security, they were rarely spoken about in relation to security. Instead, they were largely discussed in terms of product use and maintenance, or product functionality.

The DCMS Secure by Design CoP outlines what 'good' security of a consumer IoT product looks like. We found that we were able to discern information for only 5 of the 13 principles. DCMS prioritize the top three principles (CoP 1 'no default passwords', CoP 2 'implement a vulnerability disclosure policy' and CoP 3 'keep software updated') as they represent the key issues that the market needs to address immediately. We were able to derive information for all three of these key principles. For the use of default passwords, we found that—according to the material reviewed—around 4.7% of devices followed this poor practice suggesting that its prevalence in the market is not that widespread, although it is a major contributing factor in IoT botnets [29]. For vulnerability disclosure policies, only 32.4% of the sampled products had one in place. These policies are important for the security community as it allows responsible disclosure of security vulnerabilities to manufacturers. In their absence, it can mean that (discovered) vulnerabilities of IoT devices do not get fixed. Finally, for software updates, we found that for 62.4% of products, updates were discussed. However, security was discussed in only 10% of cases. Moreover, across all of the products sampled, there was no indication of how long security updates would be provided. Since this can vary across products, and is critical to their ongoing security, it is important that this information is communicated to consumers at (or prior to) the point of purchase. At present, it would appear that it is not. In short, for the devices sampled, DCMS CoP 3 was rarely addressed.

The remaining principles from the CoP were more difficult to discern as they related to storage of credentials (CoP 4), attack surfaces (CoP 6), software integrity (CoP 7), system resilience (CoP 9), the monitoring of system telemetry data (CoP 10) and the validation of data input (CoP 13). It would be unlikely for a manufacturer to disclose this information to consumers as it is not related to the maintenance of products, and so would not be obvious information to disclose in device manuals at present. Furthermore, some of this information is highly technical and so would be understood by a minority of consumers.

Perhaps most concerning is the fact that cyber hygiene advice was rarely provided to consumers, with guidance being provided for only 10% of products for which manuals or associated materials were available. In line with this, existing research has shown that the general public mainly learns about security via device prompts when they are forced to take action by a device, or through advice from family/friends [30]. In a further study, Redmiles *et al.* [31] assessed the readability of security advice provided in 1878

Table 5: A breakdown of the security features discussed in user manuals and associated materials by type of product (blank cells indicate zeros)

Product type	Total number of devices	No default password	User account management	Software or firmware updates	Factory reset or remove data	Wi-Fi encryption standard	Permission management	Local communication encryption	2FA or multifactor	Local data storage	Security of cloud	Vulnerability disclosure policy	Cyber hygiene advice	Privacy features	Screen or product lock or additional PIN	Encryption at rest	Data Encryption in motion protocol	Other type of security
Assistant	12	12	12	6	8	2		1		1		4	1		1	1	1	
Bluetooth pen	1	1	1	1	1	1		1							1			
Children's devices	4	3	3	3	2	1					1	2		1		1	1	
Exercise	1	1	1	1														
headphones	1	1	1															
Home security	28	28	26	12	9	3	6	2	1	4	4	6	5	4	2	9	10	
Light control	3			1	3							2						
Media center	5	4	4	2	3	1	1	1				4			1		1	
Pet-related	2	2	2	1			1							1		1	1	
Smart baby monitors	5	3	3	2	1	1						2	1	1		3	1	
Smart energy	11	10	10	6	7	6	2		1			2	3		4	2	4	
Smart gadgets	7	4	4	6								4			1	1	2	1
smart garden	6	5	5	3	3	3					1		1	1			1	
Smart health	6	5	5	5	5	2	1		1			2	4		1			1
Smart home monitoring	12	10	10	6	7	4	1				2	3		1	1	3	3	1
Smart kitchen	4	1	1		2											1		
smart lighting	6	4	4	5	4	3						1						
smart plug	2			2	1	1	1					2						
Smart speaker	5	3	4	4	3							2		1				
Smart transport	2	2	2												1	1	1	
Smart TV	12	5	4	12	10	5		2				9		3	8	1		
Tracker	4	3	3	2														
Wearable	31	25	25	26	13	1		1			1	10	2	4	8	2	2	1
Grand total (absolute number)	170	132	130	106	82	34	13	8	3	5	9	55	17	17	29	26	28	4
Grand total (%)	100	77	77	62	48	20	8	5	2	3	5	32	10	10	17	15	17	2

documents concerning online behaviour drawn from sources, including help pages, policies and the media. They found that in only 25 cases was the advice provided written to an adequately comprehensible standard. It is worth noting that they did not assess the extent to which the information followed the latest government guidance. Here, we focused on manuals as a source of advice and found that it was rarely given and where it was, it was not typically in line with the kind of people-centric advice provided by the National Cyber Security Centre [32]. Furthermore, the kinds of behaviour change techniques that are necessary to encourage cyber hygiene—such as 'providing information about consequences' [33]—were not employed in any of the manuals. It is well known that certain techniques (such as communications versus training) are associated with greater effectiveness and for the specific psychological constructs they seek to target (e.g. risk reception) [34, 35]. However, in the context of the IoT, further work is needed to identify the optimal behaviour change techniques for manual/support pages communications to encourage cyber hygiene behaviour, and there is a need to use a systematic approach to behaviour change intervention design [36].

At present, a consumer cannot discern the security of one device over another, which is particularly problematic during purchasing. In the absence of regulation or a labelling scheme on products, consumers have to 'research a product before purchasing' [36]. We have shown in this study that even if a consumer wanted to do such research (and if they have the technical capability to undertake it), the information is not provided to them by manufacturers. Instead, there is an information asymmetry. Consumers are therefore at a disadvantage when protecting themselves in the context of the IoT. A labelling scheme is one mechanism that could be used to communicate a device's security posture to consumers, and other work conducted as part of the PETRAS Consumer Security Index project [37] is exploring this. Another potential mechanism is for the information to be disclosed in a centralized database that has both consumer and government facing parts [23]. With respect to the information asymmetry, DCMS has recently stated that they cannot give advice to consumers about purchasing IoT devices as little information is provided about the security features of devices, whether updates are provided, and if the product warranty includes the update period [38]. Our findings support DCMS's concern and support the need for a labelling scheme to reduce this information asymmetry in security that prevents consumers from buying secure products [37].

Overall, we found that there is a lack of standardization in the communication of security-related information for IoT devices. There are no industry standards for manufacturers and the information that is currently presented in manuals and other materials depends on the manufacturer's due diligence rather than a common standard. Compare this to energy efficiency, for which manufacturers must specify an energy efficiency performance table in brochures and associated documents, and make the technical documentation available to the UK Office for Product Safety and Standards, if requested [39]. Similar standardization for the communication of IoT device security is needed to help consumers and market surveillance authorities discern the security of devices—whether this is to be disclosed in manuals, in a centralized database, or in some other way. If standardized information were disclosed in device manuals, this could be made machine readable so that information could be collated by third parties and simplified in a way that is accessible to consumers. However, this would need to be reported in a relatively standardized way to facilitate its reliable extraction.

Limitations

There are a number of limitations with the current study. First, we derived our sample from a database of IoT products and from a major UK retailer. As such, the sample largely represents products from well-known manufacturers and may not be representative of the market of consumer IoT devices, particularly those cheaper devices sold on sites such as eBay, for example.

Secondly, due to budget constraints, we could not analyse the software applications ('apps') for each of the devices. Information about security features may be communicated within the app of the device, but it was not possible to test this. However, the benefit of the current study is that it assesses publicly available information, which is representative of what is accessible to consumers prior to purchase—what we described above as the 'consumer eye view'.

Thirdly, assessing the implementation of security features through vulnerability testing was beyond the scope of this report but is an integral aspect of IoT security that we do not wish to underrepresent. This study demonstrates what information can be derived from device user manuals and support pages to give an indication of a device's security posture, but it is not the last word.

Conclusion

The manuals and support pages of consumer IoT devices do not provide adequate information about device security features. Of those that disclosed features, we were able to derive information on the top three principles from the DCMS CoP. Cyber hygiene advice is rarely provided in manuals, despite the importance it can play in preventing cybercrime. We suggest that what is communicated in manuals should be standardized and that, as suggested by Kleinhans [23], security information should be stored in a centralized repository. Doing so would aid market surveillance and perhaps, more importantly, allow device security to be summarized in a more accessible format for consumers (e.g. through a labelling scheme) to aid their purchasing choices.

Funding

This work was funded by the UK EPSRC as part of the PETRAS IoT Research Hub—Cybersecurity of the Internet of Things grant no. EP/N02334X/1 and the Dawes Centre for Future Crime at University College London.

References

1. FTC. *IoT Privacy & Security in a Connected World*, 2015. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
2. Schneier B. *Click Here to Kill Everyone*, 2017. Retrieved from http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html.
3. PenTestPartners. *WHY Is Consumer IoT Insecure?* England, UK, 2018. Retrieved from https://www.pentestpartners.com/security-blog/why-is-consumer-iot-insecure/.
4. Cisco. *Securing the Internet of Things: A Proposed Framework*. 2015. Retrieved from http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposedframework.html.
5. Veracode. *The Internet of Things: Security Research Study White Paper*, 2014. Retrieved from https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf.
6. Sadler M. *Securing Our Connected World*. 2017. Retrieved from https://dcmsblog.uk/2017/10/securing-connected-world/.

7. Hewlett Packard Enterprise. *Internet of Things Research Study 2015 Report*. 2015. Retrieved from http://fortifyprotect.com/HP_IoT_Research_Study.pdf.
8. Which?. *Could Your Smart Home be Hacked?*. 2017. Retrieved from https://www.which.co.uk/news/2017/06/could-your-smart-home-be-hacked/.
9. Loi F, Sivanathan A, Gharakheili HH *et al*. Systematically evaluating security and privacy for consumer IoT devices. In: *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy—IoTS&P '17*. 2017, pp. 1–6. Retrieved from https://doi.org/10.1145/3139937.3139938.
10. Lyu M, Sherratt D, Sivanathan A *et al*. Quantifying the reflective DDoS attack capability of household IoT devices. In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17*. 2017, pp. 46–51. Retrieved from https://doi.org/10.1145/3098243.3098264.
11. Tekeoglu A, Tosun AS. A closer look into privacy and security of Chromecast multimedia cloud communications. In: *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2015a, pp. 121–26. Retrieved from https://doi.org/10.1109/INFCOMW.2015.7179371.
12. Tekeoglu A, Tosun AŞ. Investigating security and privacy of a cloud-based wireless IP camera: NetCam. In: *Proceedings—International Conference on Computer Communications and Networks, ICCCN*. 2015b. Retrieved from https://doi.org/10.1109/ICCCN.2015.7288421.
13. Tekeoglu A, Tosun AŞ. A testbed for security and privacy analysis of IoT devices. In: *Proceedings—2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2016*. IEEE, 2017, pp. 343–48. Retrieved from https://doi.org/10.1109/MASS.2016.051.
14. Jacobsson A, Boldt M, Carlsson B. A risk analysis of a smart home automation system. *Fut Gener Comput Syst* 2016;**56**:719–33.
15. European Network and Information Security Agency (ENISA). *Security and Resilience of Smart Home Environments Good Practices and Recommendations*. 2015. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices.
16. Craggs B, Rashid A. Smart cyber-physical systems: Beyond usable security to security ergonomics by design. In: *3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS'17)*. Buenos Aires: ICSE, 2017.
17. DCMS. *Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report*. 2018a. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.
18. DCMS. *Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security*. 2018b. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774438/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf.
19. Tanczer L, Blythe J, Yahya F *et al*. *Summary Literature Review of Industry Recommendations and International Developments on IoT Security*, Department for Digital, Culture, Media and Sport, 2018.
20. PenTestPartners. *Yet Another Vulnerability in the Smarter Wi-Fi Kettle*. 2016. Retrieved from https://www.pentestpartners.com/blog/yet-another-vulnerability-in-the-smarter-wi-fi-kettle/.
21. Which? *Could My Baby Monitor Get Hacked?*. 2018. Retrieved from https://www.which.co.uk/reviews/baby-monitors/article/could-my-baby-monitor-get-hacked.
22. Jamieson A. *IoT Security—It's in the Stars!*. Retrieved from https://www.slideshare.net/AndrewRJamieson/iot-security-its-in-the-stars-169-v201605241355.
23. Kleinhans J-P. *Improving IoT Security in the EU*. 2018. Retrieved from https://www.stiftung-nv.de/sites/default/files/european_iot_product-database.pdf.
24. Gartner. *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*. 2015. Retrieved from http://www.gartner.com/newsroom/id/3165317.
25. Office for National Statistics. *Crime in England and Wales: Year Ending Sept 2016*. England, UK: Office for National Statistics, 2016.
26. Coventry L, Briggs P, Blythe JM *et al*. *Using Behavioural Insights to Improve the Public's Use of Cyber Security Best Practices*. 2014. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf.
27. Blythe JM, Lefevre C. *Cyberhygiene Insight Report*. 2017. Retrieved from https://iotuk.org.uk/wp-content/uploads/2018/01/PETRAS-IoTUK-Cyberhygiene-Insight-Report.pdf.
28. Hsieh H, Shannon S. Three approaches to qualitative content analysis. *Qual Health Res* 2005;**15**:1277–88.
29. Kolias C, Kambourakis G, Stavrou A *et al*. DDoS in the IoT: Mirai and other botnets. *Computer* 2017;**50**:80–4.
30. Redmiles EM, Kross S, Mazurek ML. How I learned to be secure: a census-representative survey of security advice sources and behavior. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security—CCS'16*. 2016, pp. 666–77. Retrieved from https://doi.org/10.1145/2976749.2978307.
31. Redmiles E, Morales M, Maszkiewicz L *et al*. *First Steps Toward Measuring the Readability of Security Advice*. 2018. Retrieved from https://www.ieee-security.org/TC/SPW2018/ConPro/papers/redmiles-conpro18.pdf.
32. Cyberaware. *Software and App Updates*. 2018. Retrieved from https://www.cyberaware.gov.uk/software-updates.
33. Michie S, Richardson M, Johnston M *et al*. The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: Building an international consensus for the reporting of behavior change interventions. *Ann Behav Med* 2013;**46**:81–95.
34. Michie S, van Stralen MM, West R. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implement Sci* 2011;**6**:42.
35. Michie S, Carey RN, Johnston M *et al*. From theory-inspired to theory-based interventions: A protocol for developing and testing a methodology for linking behaviour change techniques to theoretical mechanisms of action. *Ann Behav Med* 2016;1–12.
36. Blythe JM, Lefevre CE. *Cyberhygiene Insight Report*. 2017. Retrieved from https://iotuk.org.uk/wp-content/uploads/2018/01/PETRAS-IoTUK-Cyberhygiene-Insight-Report.pdf.
37. Blythe JM, Johnson SD. *Rapid Evidence Assessment on Labelling Schemes and Implications for Consumer IoT Security*. Department for Digital, Culture, Media and Sport, 2018. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf.
38. DCMS. *Government Response to the Secure by Design Informal Consultation*. 2018. Retrieved from https://www.gov.uk/government/publications/secure-by-design/government-response-to-the-secure-by-design-informal-consultation.
39. Department for Business Energy and Industrial Strategy. *Regulations: Energy Information—Guidance for Suppliers and Dealers*. 2018. Retrieved from https://www.gov.uk/guidance/the-energy-labelling-of-products#how-do-i-comply.

Appendix

Table A1: Glossary of terms

Abbreviation	Term	Definition
2FA	Two factor authentication	A method for authenticating a users' identity using two different factors. These can include something they know (e.g. a password), a physical possession (e.g. a USB key or bank card), or factors associated with the user (e.g. biometrics). App generated codes are another example.
AES	Advanced encryption standard	Is a cryptographic algorithm used to encrypt or secure data. It uses a symmetric-key block cipher algorithm (which can be used encrypt and decrypt data) and has cryptographic key sizes of 128, 192 and 256 bits. The larger the bit size, the more secure the data.
API	Application programming interface	A set of subroutine definitions, communication protocols and tools for building software applications (including websites) that interact with one another.
DDoS	Distributed denial of service	A method of cyberattack for which the perpetrator seeks to make a targeted machine or network resource unavailable by flooding (or overwhelming) it with traffic from many different sources.
Digital certificate		An electronic document, signed by a certificate authority, which verifies the identity of an individual, an entity or a company owning the website/app on the Internet.
FHSS	Frequency-hopping spread spectrum	A method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both the transmitter and receiver. The aim is to make the signal resistant to interception.
Hard-coded password		A practice of embedding a password directly into the source code of a programme or other executable object, making it permanent.
HMAC	Hash-based message authentication code	A method used to simultaneously verify both the data integrity and the authentication of a message sent between two systems.
HTTP	Hypertext transfer protocol	Hypertext transfer protocol for communication over a communication network without encryption.
HTTPS	Hypertext transfer protocol secure	An extension of HTTP for 'secure' communication over a computer network. HTTPS uses SSL or TLS to encrypt the data.
PKI	Public key infrastructure	With PKI, a public key is used to encrypt data and a private key is used to decrypt it.
SSL	Secured sockets layer	A standard security technology for establishing an encrypted link between two systems (typically a server and a client).
TLS	Transport layer security	An updated and more secure version of SSL.
WAC	Wireless accessory configuration	Apple's licensed technology designed for accessories that connect to iPod, iPhone and iPad without requiring the user to type in the network name and password.
WEP	Wired equivalent privacy	An early generation of security protocols for protecting wireless communication.
WPA	Wi-Fi protected access	A security protocol for protecting secure wireless communication. WPA was introduced after WEP and is more secure.
WPA2	Wi-Fi protected access II	A security protocol for protecting secure wireless communication. WPA2 was introduced after WPA and is more secure as it uses more advanced encryption.
WPS	Wi-Fi protected setup	A network security standard to create a secure wireless home network. It is considered less secure than newer standards, such as WPA and WPA2.
Z-wave		A wireless communication protocol, using low-energy radio waves for home automation. It allows home appliances, such as IoT devices to communicate with each other.