Alec Blanton and Eddie DeMars

CSCI-B 433

Dr. Luyi Xing

2 May 2023

How to Inform Consumers of their Devices' Privacy: A Survey of IoT Privacy and Security Labelling

1 Introduction

As more and more devices around the world connect to the internet, it is inevitable that some of them will insecure against attacks. These Internet of Things (IoT) devices are owned by approximately 70% of consumers, and that number will only continue growing [1]. As such, it is important to ensure that these devices are able to protect their users' security and privacy, but many are currently unable to do so. For example, a paper comparing the security properties of two common IoT hubs (the Samsung SmartThings Hub and Sen.se Mother) found that both of them were severely lacking in many areas that would be considered best practices within the industry [2]. Alongside securing individual products, what is equally as important is informing consumers of whether their devices are secure. If devices are secure but consumers do not know it, they may not be able to trust their devices. If devices are insecure but consumers do not know it, they may put trust in devices that they should not. And if two devices have different security properties but consumers do not know it, they may be unable to compare the two devices and decide which is better for them. So how can we inform consumers about IoT device security and privacy?

The answer lies in labeling. If an effective scheme to label devices based on their various security and privacy properties, then consumers can better make decisions about their purchases. In addition, this would put pressure on manufacturers to create more secure devices and to better protect consumers' privacy, as consumers would be less likely to buy their products if they do not.

There are two main problems within the security labeling area of study:

1) Creating security labels for IoT devices takes resources and effort on behalf of IoT manufacturers.
2) Customers who are not experts in Information Security need to be able to understand the security labels

A study conducted by Carnegie Mellon found that consumers "... preferred purchasing a smart device with no security or privacy information compared to a smart device with least protective label." [7]. This means that IoT producers who follow the (currently optional) labeling guidelines will only do so if security is a major selling point of the device - and those are not the devices the IoT label is being made for. While consumers will react negatively to a label that gives poor reviews, they will simply not react to a device that doesn't have a simple label because that has always been the status quo. The study found that "...when security and privacy information was not mentioned, participants assumed that the device's practices were not that risky" [7]. In order to meet certain criteria for either the Carnegie Mellon model or the Singaporean model, IoT developers will need to invest significantly more money into the production cycle for things like third-party assessments and penetration testing. This will increase the costs of research and development for devices, which will likely be offset by increasing devices' price tags at the store.

Currently, figuring out whether or not an IoT Device is secure requires deep knowledge of Cybersecurity principles themselves. The average consumer will not know the different encryption algorithms or if 6 months is a reasonable amount of time for security updates to be patched through. Even a sticker like "NIST Approved!" does not convey all that much information - the average consumer has probably never heard of the government agency because they do not interact with the average American citizen at all. Additionally, if a security breach develops, it is not feasible to reprint all of the labels on every existing IoT device. There must be a way to update the label, such as an online link. A security label needs to be designed much in the same way a nutrition label is designed: it should give easy-to-digest information from a trusted authority for the average consumer to understand so they can make the choice that is best for them.

2 Approach

The bulk of this paper will be in section 3, where will go through a brief history of privacy and security labeling then move on to some examples of schemes, both in-use and theoretical. We will discuss the primary features of each of these possible schemes and then talk about a possible pitfall in choosing criteria for labels. In section 4 we will put forth our own suggestions for our ideal labeling scheme, mixing the best ideas of all the examined proposals and trying to solve their issues. Section 5 will consist of a summary of our findings as well as any final conclusions, and section 7 will contain any sources cited.

3 Survey of Existing Techniques

3.1 History

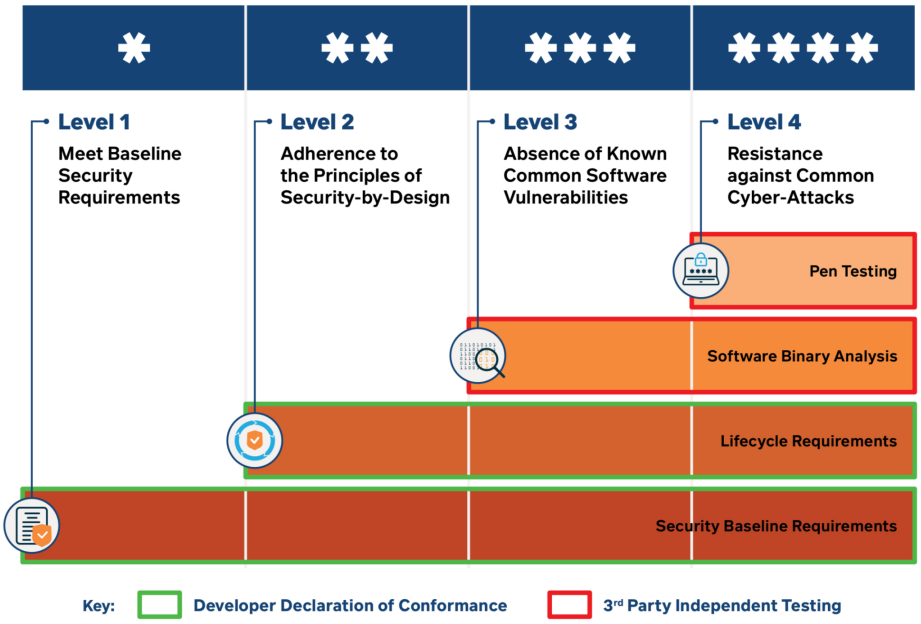
In the final days of 2020, Apple introduced its software privacy labeling requirements in the Apple store [3]. Software Security labels are mandated by Apple to inform users of what information applications track from them - things like PII, location, hardware specifications, and more are some of the many things they inform users about. These labels provide easily digestible information to consumers to help them better protect their privacy. Apple made this effort voluntarily, as opposed to being mandated by a government body, in the hopes of getting ahead of EU regulations.

One of the simplest labeling schemes currently in use is the BSI Kitemark for IoT devices in the UK[1]. The British Standards Insititute is a well-respected organization within the UK and the Kitemark has widespread recognition amongst the British public[1]. The Kitemark is extremely simplistic, simply having its logo and the setting in which it is supposed to be used (residential, commercial, or enhanced)[4].

BSI Kitemark for IoT Devices[4]

Only a select few nations have any legally binding guidelines for informing consumers about the privacy practices of devices. One of the most recent nations to do so is the UK, which released informal guidelines back in 2019 after a research group found that the average UK home had 10 smart devices [9], with more formal regulations being pushed through in late 2022 [10]. These regulations, also known as the Product Security and Telecommunications Infrastructure Bill, provide a checklist of requirements, such as breach and security update lifecycle disclosure, which apply to most IoT devices - smartphones, home assistants, baby monitors, home cameras, etcetera. That being said, this is just a checklist of things that companies must now do before their products come to market - and may not be all-encompassing.

Another proposal by the Singaporean government uses a simplistic four-star scale to rate IoT devices using the following criteria on the following chart [7]. The purpose of this system is to inform consumers about the security of their IoT devices, with one star demonstrating that the device follows all legal requirements, and nothing more, and four stars showing that the device goes above and beyond to make sure the device is secure. Germany and Finland have an even simpler version of the CAS (Cyber Security Agency) of Singapore's guidelines - providing an effective check-mark for anything that passes level 2 of the CAS guidelines [8]. All nations mutually recognize the other's cybersecurity labeling.

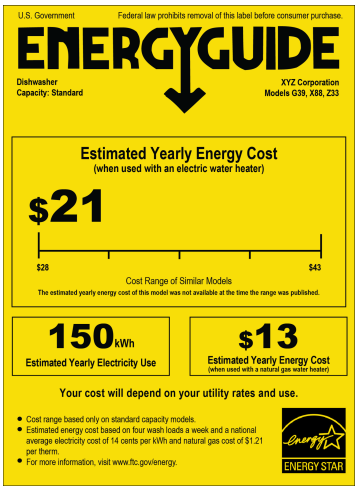


The Singaporean Government four-star rating scale of IoT Devices [7]

3.2 Today

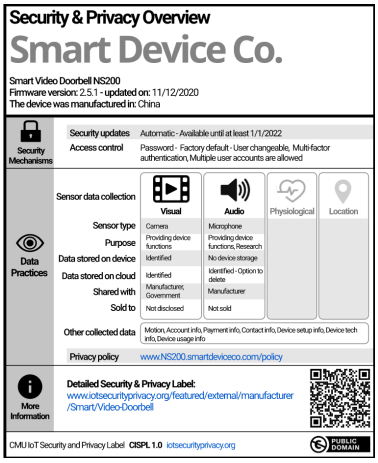
In the US, the NIST was tasked with proposing guidelines by Spring of 2023, and they have - technically- followed through [11]. In 2021**,** the NIST released a white paper detailing what they would like to see for IoT Security Labels [14]. While all of the following proposals look only at Asset Configuration specifications (i.e., default password usage and the ability to opt out of features), the proposed label also recommended instituting physical identifiers and making physical alterations to the device. Another unique aspect of the NIST plan was to analyze devices based on aspects other than direct device configuration and policy. The NIST plan also wanted to look at standardizing Documentation so it would be easier to detect and patch security fixes. According to the security corporation Digicert, the US is expected to release optional guidelines for IoT Devices to accurately label themselves sometime this spring [6]. The NIST has released guidelines of what a security label *should ideally* have on it, but there have been no mandatory regulations created yet. In a press release at the end of 2022, the White House stated that they would take inspiration for this new cyber security label from the Energy Star program under the Environmental Protection Agency (EPA) [12]. The Energy Star Program provides a label that

describes the energy efficiency of devices, however, this is an opt-in program and strict criteria must be met before a company qualifies to partner with the Energy Star program. The following is an example label to show what kind of information this provides:



An Example of an Energy Star Guideline [13]

There are many other proposals for security labels in the works already. One promising research group from Carnegie Mellon has conducted studies with both experts and consumers verifying the demand for better information from tech-literate consumers [5]. This group conducted extensive research (n=737) to determine whether consumers were able to accurately define their identifying categories (i.e, “No Cloud Storage”) on the proposed nutrition label. The study ascertained many other useful pieces of information about privacy labels on IoT devices. One such revelation was that consumers, both experts and laymen, were more likely to purchase a device without a label than a device with a label warning them about poor device safety practices.



The “Security Nutrition Label” example developed by researchers from Carnegie Mellon [5]

Looking at the example label from Carnegie Mellon, it is possible to see how different two different labels can be. Rather than the simplistic star-based approach of Singapore, the Carnegie Mellon label has a lot more information on both the security and privacy details of the product[5]. On the security side, we can see that it includes how it will receive security updates and how it handles access control. On the privacy side, we can see what it does with various types of personal data, including what kind of data is and is not collected, why it is collected, where and how it is stored, who it is shared with, and who it is sold to, as well as a link to their privacy policy. Finally, perhaps the most innovative, it includes a QR code and URL to an external site with more in-depth and up-to-date information, allowing for more technical users to look at more advanced information and for all users to see if all of the information on the label is still up to date or perhaps if the product or company had a privacy leak.

3.3 Potential Issues With Basing Labels Off a Checklist

Device security is often viewed as a sort of checklist. If all the right boxes on the list are checked, then a device is secure. If it is missing some, it is slightly insecure. If it is missing a lot, very insecure. This method has some merit as it provides a simple way to analyze the basic security properties of a given device. As shown in the paper *Best Practices Would Make Things Better in IoT*, which compares the security and privacy properties of two different IoT hubs, it is very easy to go through a checklist and list

whether or not a given device satisfies the criteria [2]. However, also shown in that paper is why this is unsatisfactory. Both hubs were extremely insecure, but the ways in which they were insecure matters.

When looking purely at how many criteria each hub passed (i.e. unconditional yes's in a category), Samsung had 20 and Sen.se had 14 out of 40 [2]. This would give the Samsung hub a 50% and Sen.se a 35% on a system based purely on how many boxes were checked. However, the security properties were much more different than these results would indicate. For example, the researchers were able to inject messages into and alter outgoing messages from the Sen.se hub but were unable to do so for the Samsung hub, making the difference much worse than the 6 points would indicate in our opinion.

As well as not all criteria being equal, it is possible for a certain product to technically fulfill a criterion but for the given feature to not meaningfully contribute to security. For example, the paper notes that the Samsung hub does technically provide transport security, however, it is reliant upon SHA-1, which is considered to be broken and insecure[2]. Sen.se does a similar thing, establishing a TLS connection, but not using it to send and receive data, instead using insecure HTTP[2]. Given all of this, any labeling schema that relies solely on a binary checklist would have some major issues, as it would be possible for insecure devices to be labeled as secure if used carelessly.

4 Suggestions

A good labeling scheme would take the best elements of all the aforementioned schemes to create something easily understandable to the layman while still giving enough information to be useful. The scheme we believe to be the most useful is the one proposed by Carnegie Mellon. The scheme presents plenty of information while not being too technical[5]. We also liked the idea of having a QR code or URL link to a website that would have more up-to-date and thorough information, which would be important if the security details of a product have changed. However, we do have concerns that it may have too much information and potentially overload a consumer reading it. There is also no easy way to quickly compare two products' security and privacy levels beyond reading the individual features on the label.

Some of this can be fixed by taking inspiration from the Singapore labeling scheme. While we believe that the scheme is overall insufficient due to not having enough information, having a quick and easy star-based system to compare two different products is very convenient for the consumer[7]. This way a consumer can see that one product has 3 stars and another has 4 stars and make an informed decision rather quickly. When combined with the more thorough information and link to an external site for even more information from the Carnegie Mellon label, we believe that an extremely effective labeling scheme could be developed.

Of course, a labeling system is more than just what goes on the package. It is important that the criteria being used for the labels are fair and effective. The safety features used to pass a given criterion need to have an actual meaningful impact on the security of the device, and as such inspections and tests need to have advanced criteria that are able to look deep at the security of a device. As one paper put it "simply having a Boolean requirement is not adequate" [2]. These requirements should also be updated regularly to reflect changes in the security landscape.

The way the labels are awarded also needs to be handled carefully. Ideally, they would be handled by a government agency that could potentially allow certain third parties to act as auditors. Whoever is in charge must also be willing and able to remove stars from a label if a company is found to no longer be compliant with their security level and potentially even punish a company that lied to achieve a higher level.

Following up on this, we believe that for a labeling scheme to be successful it must be government-backed and mandated. While there has been some success seen in labels handled by private companies, we do not believe that these will be sufficient, because as said previously, consumers are more likely to buy products with no label than bad labels [5]. On the other side of things, we believe that the labels do not need to look at things that would not directly affect the consumer, such as the documentation methods. As such, companies that would receive bad labels would simply not put them on their product and consumers may be none the wiser. This would not happen if labels are government-mandated, as companies would be forced to put the labels on their products, even if they were not favorable.

Perhaps most important is that a labeling scheme exist. Almost any labeling scheme is likely better than none. Even the most simple, optional label that tells consumers nothing other than “this is secure in some way” is better than nothing. This way consumers have something they can easily look at to know a product will be secure. While it is important that a label is good, and labels should not be recklessly mandated without any thought, it is also important that bodies such as NIST actually release schemes for use in a timely manner.

5 Conclusions

This paper looked at the potential use of privacy and security labels as a way to better inform consumers of the safety of the products they are buying and to pressure the IoT industry to have better privacy and safety standards. An effective labeling scheme would allow consumers to easily and quickly compare products to find one that was right for them as well as force producers to create products that protect their customers’ data since any that do not will have their poor security put on full display to consumers.

We looked at various already existing schemes such as Singapore’s, which relies upon a four-star rating system where one star demonstrates that the device meets the bare minimum legal requirements and nothing more, and four stars means going above and beyond[7]. We also looked at some theoretical frameworks, such as what little we know about the NIST framework slated to come out that takes inspiration from Energy Star guidelines[13] and their older proposals that would include requirements . Another one was proposed by researchers at Carnegie Mellon, who put forward a scheme that included basic security and privacy features of the product alongside a QR code to get more in-depth and up-to-date information[5]. We also looked at why it is important to not use a simple binary checklist when assigning grades to products.

We put forth our own suggestions for an ideal privacy and security labeling scheme. We believe that an ideal scheme would be closest to the one put forth by the Carnegie Mellon researchers with the addition of a rating system similar to that of Singapore. In addition, we believe that any labels need to be based on clear but careful criteria and that labels need to be assigned by a non-biased party with

government backing. Labels should also be government-mandated on all relevant products to ensure they will actually be used.

6 References

[1]Badran, H. (2019). IoT Security and Consumer Trust. Proceedings of the 20th Annual International Conference on Digital Government Research, 133–140. https://doi.org/10.1145/3325112.3325234

[2]Momenzadeh, B., Dougherty, H., Remmel, M., Myers, S., & Camp, L. J. (2020). Best Practices Would Make Things Better in the IoT. IEEE Security & Privacy, 18(4), 38–47. https://doi.org/10.1109/MSEC.2020.2987780

[3] Perez, S. (2020, December 14). *Apple launches its new app privacy labels across all its App Stores*. TechCrunch. https://techcrunch.com/2020/12/14/apple-launches-its-new-app-privacy-labels-across-all-its-app-stores

[4]BSI launches Kitemark for Internet of Things devices. (n.d.). Retrieved May 2, 2023, from https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-internet-of-things-devices/

[5]Are Consumers Willing to Pay for Security and Privacy of IoT Devices? Pardis Emami-Naeini* , Janarth Dheenadhayalan† , Yuvraj Agarwal† , Lorrie Farith Cranor†

[6] *U.S. Efforts Underway for IoT Security Labels by Spring 2023 | DigiCert*. (n.d.). Www.digicert.com. Retrieved May 2, 2023, from https://www.digicert.com/blog/iot-security-labels-by-spring-2023

[7] Purdy, K. (2022, October 20). *Everything we know about the White House's IoT security labeling effort*. Ars Technica. https://arstechnica.com/gadgets/2022/10/everything-we-know-about-the-white-houses-iot-security-labeling-effort/

[8] *Singapore, Germany to mutually recognise IoT cybersecurity labels*. (n.d.). ZDNET. https://www.zdnet.com/article/singapore-germany-to-mutually-recognise-iot-cybersecurity-labels/

[9] May, S. (2022, November 8). *The upcoming UK IOT Security Law: What you need to know*. Evalian®. Retrieved April 14, 2023, from https://evalian.co.uk/the-upcoming-uk-iot-security-law-what-you-need-to-know/

[10] plc, A. (2020, January 15). *Tech Nation: Number of internet-connected devices grows to 10 per home*. Aviva plc. Retrieved April 14, 2023, from https://www.aviva.com/newsroom/news-releases/2020/01/tech-nation-number-of-internet-connected-devices-grows-to-10-per-home/

[11] Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software. (2021). *NIST*. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0

[12] Page, C. (2022, October 19). *US to launch "labeling" rating program for internet-connected devices in 2023*. TechCrunch. https://techcrunch.com/2022/10/19/us-cyber-label-routers-smart-speakers

[13] Hebert, A., Hernandez, A., Perkins, R., & Puig, A. (2022, November 1). *How to use the EnergyGuide label to shop for Home Appliances*. Consumer Advice. Retrieved April 30, 2023, from https://consumer.ftc.gov/articles/how-use-energyguide-label-shop-home-appliances

[14] *DRAFT Baseline Security Criteria for Consumer IoT Devices*. (2021). https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%20202021-08-31.pdf