Comments on "Establishing Confidence in IoT Device Security: How do we get there?"

Pardis Emami-Naeini
University of Washington
pardis@cs.washington.edu

Yuvraj Agarwal
Carnegie Mellon University
yuvraj@cs.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cmu.edu

The NIST white paper identified the IoT label as a potentially effective mechanism to instill confidence in IoT device security. In what follows, we would like to emphasize the importance of designing usable and informative IoT labels by highlighting the key findings of our research and peer-reviewed publications on this topic. We first provide a brief summary of the journey of designing the label. We will then focus on how our designed label can fill the gaps that we identified in the NIST white paper. The research described in this document has been conducted at Carnegie Mellon University, Pittsburgh, PA.

We conducted a series of interviews and surveys with consumers of IoT devices. We found that consumers do not have privacy and security information readily available to them when making purchase decisions, but often become concerned about privacy and security after purchasing IoT devices [1]. We then decided to design a label for smart devices to provide such transparency for consumers.

To specify the information that should be included on the label, we recruited a diverse sample of privacy and security experts from academia, industry, government, and NGOs. Through a series of in-depth interviews with experts, we identified 47 pieces of information to include on the label. To fit this information, we designed a layered label, with two layers: primary and secondary. The primary layer is the concise, consumer-friendly format of the label that can be printed and attached to the package of product. The secondary layer is the detailed online version of the label that can be accessed by scanning the QR code or typing in the URL included in the primary layer [2]. In addition, the online version of the label has computer-readable metadata (JSON and XML), allowing for automated processing by search engines, comparative shopping tools, and other automated tools.

In addition to the label, we designed a tool to facilitate the label generation process. By using the tool, manufacturers can fill out a form for each section of the label and see the label being generated in real time. They can also save the JSON or XML format of the label and then resume working on it at a later time. More information about our label and the tool is available on our website [1].

To test the effectiveness of the designed label, we conducted a large-scale online study and measured the efficacy of the label in conveying risk to consumers and impacting their desire to purchase smart devices. We found that almost all of the information presented on primary layer of the label is successfully communicated to consumers, although some

[1] https://iotsecurityprivacy.org/

attributes (e.g., internal and external audits) need to be further explained [3].

Label covers both security and privacy of IoT devices. Through extensive surveys and interviews with consumers of IoT devices and privacy and security experts, we designed a label that informs users about both security and privacy features of IoT devices.

Page 4 of the white paper identifies some of the challenges to implementing and maintaining strong IoT security. One of these challenges is to communicate with consumers regarding new security vulnerabilities as well as firmware/software updates. On the primary and secondary layers of our label we included the attribute *security updates* to specify whether and in what way the device receives security updates. This factor can take levels such as automatic, manual, or consent-based. In addition, we included an attribute called *vulnerability disclosure and management*, which among other information, provides users with the history of known vulnerabilities and their patch status. As mentioned in the white paper, the security posture of IoT devices depends greatly on the firmware of the device. We mention the firmware version of the device on both the primary and secondary layers of the label.

Software-bill-of-material was another security attribute that was mentioned on page 14 as an important piece of information to be communicated to the users. In fact, recent work shows that the use of third party libraries in IoT device firmware is quite common, similar to the use of libraries in traditional software development. More importantly, many of these libraries are often left un-patched for long periods by IoT device manufacturers (even years) despite critical security vulnerabilities being disclosed and made available by the library developers [4]. Providing a Software-bill-of-material can help secure such unpatched devices and be a forcing function for manufacturers to provide regular firmware updates. To provide this information, on the secondary layer of our designed label, we included a factor called software safety. The reason we included the factor on the secondary layer as opposed to the primary layer was that in our studies, a small subset of consumer participants asked us to have this information on the first layer whereas most were interested in having access to this information on the secondary layer.

While recognizing privacy and safety as two key pillars of trustworthiness for cyber-physical systems, the white paper is primarily focused on confidence mechanisms related to the security of IoT devices. The unknown sensitivity of the collected data was identified as one of the challenges of implementing security confidence for IoT devices. From media reports, we already know that manufacturers are not always transparent about the sensing capabilities of their devices, let alone the sensitivity of the collected information [5, 6]. On the privacy section of our label, we ask manufacturers to disclose the types of sensors their devices have and the data practices related to each sensor type (e.g., purpose of data collection, who the data is being shared with and sold to).

Label is designed through a user-centric process. A critical piece that is missing from the white paper is the discussion around designing a user-centric label as a confidence protocol. Confirming our research findings [1], on page 18 of the white paper, it is mentioned that the information about the privacy and security of smart devices is not easily accessible to IoT consumers at the time of purchase. It is also mentioned that even if the information is available to them, it is not clear to what extent consumers can understand it. We focused on consumers when designing our labels to make sure the designed label effectively communicates the information and conveys risk to consumers. We achieved this by involving consumers from the very beginning of the design process and iteratively improving the content and design of the label to make it understandable and informative to consumers.

Online version of the label can be updated. On page 4 of the white paper, highly configurable software/firmware of IoT devices is listed as one of the challenges in implementing and maintaining a strong security posture. To accommodate the need to update the privacy and security practices throughout the lifetime of the product, we designed our label to have an online version (i.e., secondary layer) in addition to an optional printable version (i.e., primary layer), both of which include the specific version of the firmware that the label refers to.

Implementing secure defaults is not enough. Theme 5, on page 17 of the white paper, mentions that individual customers of IoT devices should not be expected to able to consider privacy and security information to make an informed purchase decision. Therefore, manufacturers should provide strong default security capabilities for IoT devices to help IoT consumers. We agree that as a best practice, IoT manufacturers should implement protective default privacy and security practices for their products. However, our research has shown that providing secure defaults is not enough for consumers.

When measuring the effectiveness of our label content, we found a few misconceptions related to some of the security attributes on the label [3]. For example, to some participants, the availability of security updates is a sign of bad security due to the very need of the device to get updated. To mitigate such misconceptions, manufacturers could provide additional information explaining why a specific privacy or security practice is implemented and how the practice protects the user from the risks. Our designed label facilitates providing useful additional information about privacy and security practices. Such additional information can be accessed by clicking on the plus signs that are placed in front of the privacy and security attributes on the secondary layer.

Multi-factor authentication (MFA) is another example, showing how to some consumers, a secure practice does not translate to an increased desire to purchase the device. Some of our participants reported that due to the inconvenience and usability challenges of MFA, they would be less interested in purchasing a device that has such an authentication protocol. Similarly, not all consumer participants were interested in automatic security updates, despite it being a security best practice. Some of our participants reported that they would like to have autonomy over security updates, therefore they would prefer manual updates over automatic updates. Our user-centric research indicates that secure defaults would not be welcomed by consumers unless they are usable and provide users with some autonomy to control the behavior of their device. On our label, the available controls for each of the privacy (e.g., option to opt out) and security practices (e.g., user changeable password) of the device will be presented in front of the practice.

References

[1] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[2] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 447–464, 2020.

[3] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. Faith Cranor. Which privacy and security attributes most impact consumers' risk perception and willingness to purchase iot devices? In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1937–1954, May 2021.

[4] Han Zhang, Abhijith Anilkumar, Matt Fredrikson, and Yuvraj Agarwal. Capture: Centralized library management for heterogeneous iot devices. In *USENIX Security Symposium*, 2021.

[5] Alfred Ng and Megan Wollerton. Google calls Nest's hidden microphone an "error". https://www.cnet.com/news/google-calls-nests-hidden-microphone-an-error/, February 2019.

[6] Carrie Mihalcik. Apple HomePod Mini reportedly has a secret sensor for temperature, humidity. https://www.cnet.com/home/smart-home/apple-homepod-mini-reportedly-has-a-secret-sensor-for-temperature-humidity/, March 2021.