IoT Security and Privacy Labels

Yun Shen[1(✉)] and Pierre-Antoine Vervier[2]

[1] Symantec Research Labs, Reading, UK
{yun_shen,pierre-antoine_vervier}@symantec.com
[2] Symantec Research Labs, Sophia Antipolis, France

Abstract. IoT devices are riddled with vulnerabilities and design flaws. In consequence, we have witnessed the rise of IoT specific malware and botnets with devastating consequences on the security and privacy of consumers using those devices. Despite the growing attacks targeting these vulnerable IoT devices, manufacturers are yet to strengthen the security posture of their devices and adopt best-practices and a security by design approach. To this end, we devise an concise, informative IoT labelling scheme to convey high-level security and privacy facts about an IoT device to the consumers so as to raise their security and privacy awareness.

1 Introduction

The Internet of Things (IoT) market has taken off. There are hundreds of thousands of connected IoT devices available for the consumers ranging from fitness tracking devices, security webcams to smart home appliances. However, despite their increasing acceptance by consumers, recent studies of IoT devices [5] demonstrated that "security" is not a word that gets associated with this category of devices, leaving consumers potentially exposed to massive attacks [24]. In consequence, we have witnessed the rise of IoT specific malware such as Mirai [1], Brickerbot [7], Tsunami [8] and a series of high profile incidents involving IoT devices in recent years [10].

Common mistakes that we have seen in these devices that lead to the aforementioned incidents include the use of unencrypted network communications, hardcoded username/password (which is prone to brutal force attack), lack of strong authentication mechanism, etc. For example, Symantec reported that almost two out of ten mobile apps used to control the tested IoT devices did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. That being the case, it is inevitable that attacks on Internet of Things (IoT) devices will increase dramatically due to the accelerated growth in the number of internet-connected smart devices/appliances without security by design.

It is important to note that most IoT devices are closed, i.e., their software and hardware designs are proprietary. In addition, most of these devices have limited processing capability and storage capacity. These factors render conventional security techniques less feasible. For example, customers cannot install

M. Naldi et al. (Eds.): APF 2019, LNCS 11498, pp. 136–147, 2019.
https://doi.org/10.1007/978-3-030-21752-5_9

additional security software into these devices like what they could do with PCs. Given the close coupling of hardware and software in the IoT model, one approach to strengthen the security posture in the IoT is "security by design", where security is built into IoT devices so that they are secured at various system levels. For example, IoT device makers should require encryption and authentication for devices to know whether or not they can trust a remote system. Depending on the processing capability of a device, they can also leverage host-based protection to provide various security functionalities including hardening, lockdown, whitelisting, sandboxing, network facing intrusion prevention, etc.

Another important aspect relating to IoT security is the end users. Most IoT devices are designed to provide the end-users with a small number of functions to accomplish a specific goal, e.g., fitness tracking, remote monitoring, etc. In turn, they offer a limited user interface. Lacking of keyboards or effective input mechanisms, the device makers are prone to take shortcuts and make the implementation of authentication mechanisms weak by default, for instance, by hindering or preventing the update of the password in a password-based authentications. Rooting upon the aforementioned 'closed' characteristic, the end users are not always aware of the cybersecurity risk associated with a given IoT device, nor there exists any standardized format/metrics to inform the end users about such risk. In many cases, well informed consumers are capable of understanding the threat posed by IoT devices. For example, after the Mirai attack, considerable number of consumers changed default passwords of these affected devices and reduced the risk of compromise.

The question that motivated our work is: "can we devise an concise, informative format to convey high-level security and privacy facts about an IoT device to the consumers?" To address this question, we developed a security and privacy label for IoT devices to improve consumers' purchasing decisions. "Nutrition Facts" label was designed by the FDA to reveal sources of information as to the contents of food. From this label we can ascertain the breakdown of ingredients including fat, carbohydrates, vitamins etc., and some crucial information such as allergy advice, dosage. *So what factors would go into a security and privacy label for IoT devices? How should we organize these factors so that they can easily be understood by consumers*, especially in light of the new best-practice recommendations [17] published by ENISA in 2017?

2 Related Work

IoT security and privacy label is a relatively new idea. In this section, we aim to review all related work in the literature.

Kelley *et al.* [18] is one of the very first research effort on designing a privacy label which presents to consumers the ways organizations collect, use, and share their personal information. Centering on the goal to create an informational design that improves the visual presentation and comprehensibility of privacy policies, the authors iteratively experimented with three privacy label designs: Platform for Privacy Preferences (P3P) expandable grid, P3P simplified grid and privacy nutrition label. They performed a 24-participant laboratory user

study comparing a standard natural language privacy policy with privacy policies presented in their privacy nutrition label. The experimental results demonstrated that the participants using the privacy nutrition label design could consistently select the companies that had strong privacy policies, in contrast to those using natural language privacy policies.

Following this effort, Kelley *et al.* [19] carried out an online user study of 764 participants on testing five privacy policy formats: standardized table, standardized short table, standardized short text, full policy text, and layered text. Note that the first two designs are inherited from Kelley *et al.* [18]. The authors crafted seven blocks of questions (e.g., single policy likability, policy comparison likability, etc.) to study the effectiveness of these five designs. Based up on the experimental results, the authors concluded that policy formats do have significant impact on users' ability to both quickly and accurately find information, and on users' attitudes regarding the experience of using privacy policies. The authors claimed that the standardized table and standardized short table overall outperformed the rest of the designs.

More specifically, for IoT devices, there is a need for transparency, control, and new tools to ensure that individual privacy requirements are met. Therefore, it is important to better understand people's perception on the privacy implications of using IoT devices and how they prefer to be notified about data collection [21]. To this end, Naeini *et al.* [20] conducted a 24-participant semi-structured interview study followed by a 200-participant MTurk survey to study consumers' knowledge, and pre- and post-purchase behavior regarding IoT security and privacy. The authors revealed that security and privacy were factors that would influence consumers' purchase decisions if IoT devices may collect sensitive information. Building on top of these survey results, the authors also evaluated a prototype privacy and security IoT label. In addition to the conclusions presented in [18,19], the authors observed that such IoT security and privacy labels need to be widely used and convey accurate information (e.g., definitions of the terms). Additionally, an interactive online label can be helpful for the users to obtain additional information.

These previous literature leans toward privacy policies, explaining how data would be collected, used and shared. However, privacy should not be considered as a standalone factor when designing such an IoT label. For example, a security flaw of an IoT device can lead to private information leakage. Based on previous research on attacks against IoT devices as well as on system-level IoT device security, our work embraces a holistic approach to devise an concise, informative format to convey high-level security and privacy facts about an IoT device to the consumers.

3 Design of Security and Privacy Labels

As we have seen in the previous Section, both consumers and the cyber security and privacy actors have expressed the need for independent quality metrics, *à la* "food nutrition facts" for IoT devices. We refer to these as "IoT facts" in the

reminder of this document. Designing such device factors is a delicate process, which brings up several challenges.

- The first challenge consists in **defining** the device factors and associated terms, taking into account that they need to convey an *concise and informative* yet complete *security and privacy* assessment of an IoT device to the consumers.
- The second challenge is related to the **implementation** of the device factors. In order for consumers to rely on device factors in the buying process, these factors must be *accurately* set and properly kept *up-to-date* throughout the device lifetime. It must also be possible to *verify* the correctness of these factors. Given the high heterogeneity in IoT devices hardware and software, developing techniques to profile and accurately extract detailed information about these devices is a challenging task, which requires further research.

In the reminder of this section (i) we present a list of device factors that concern consumers the most, (ii) we propose two layouts to visualize these device factors, and (iii) we elaborate on the existing and potential, yet to be researched, new techniques to populate and verify the device factors.

3.1 Device Factors

Considering the fact that most consumers don't have excessive knowledge in technology, it is vital for the proposed security and privacy factors to capture the essential factors that may offer the most assistance to consumers' purchase decision. Additionally, these factors must reliably reflect the device's resilience to cyber attacks as well as its ability to keep the consumer's data safe. To this end, we propose five label categories: (i) *system (security)*, (ii) *communication (security)*, (iii) *sensory (privacy)*, (iv) *data (privacy)* and (v) *connectivity (information)*.

System (Security). This category gives a basic set of guidelines to consumers to consider from their perspective in terms of device security. These fundamentals will greatly improve the consumers' security awareness of any IoT product. For example, this category will cover if a device has (in)sufficient authentication, or if a device uses encrypted communication when backing up data, secure firmware/OTA update, etc. A list of factors within this category is shown below.

- *Certificates:* certifications granted to the device by 3^{rd} party certification authorities;
- *Secure boot:* prevents booting from a unsigned/modified device firmware;
- *Firmware/software update:* describes the device's supported firmware update methods;
- *Password:* characteristics and update mechanisms of potential passwords used;
- *Authentication:* available authentication mechanisms when accessing the device;

- *Remote Access:* device's ability to be accessed remotely, for instance via an application on a mobile phone, from the home network or the internet.

Communication (Security). One of the most interesting features for consumers is the ability to directly interact with IoT devices they deploy on their home network through network communication channels. Unfortunately, this feature also creates an attack vector for cybercriminals. IoT devices' capabilities to secure their communication is thus key to preserving users privacy and devices security. We provide the list of factors for this category in the list below.

- *Encryption:* whether the network communications involving the IoT device are encrypted and the characteristics of the encryption used;
- *Internet access:* whether the device requires access to the Internet to work properly;
- *Talk to other devices:* whether the device is intended to communicate with other devices on the local network.

Data (Privacy). Privacy is one of the most important factors in terms of IoT devices. The motivation behind this category is that the proposed device factors should inform the consumers if any personal information/anonymous diagnostic data is collected by an IoT device; if any local/remote data storage is supported by this device, etc. The list of considered factors within this category is shown below.

- *Personal information:* informs whether personal information is collected by the device and, if yes, describes the type of information;
- *Telemetry data:* informs the user whether anonymous telemetry data, such as usage statistics or threat monitoring alerts, is collected and potentially reported back to the manufacturer;
- *Data storage:* describes the different types of storage supported and used by an IoT device so that the user is aware of where the data is stored, if policy guarding the data storage is GDPR compatible, etc.

Sensory (Privacy). In general, a sensor is an electronic component designed to detect events or changes in its environment and send the information to other electronics. With advances in micro-machinery and easy-to-use microcontroller platforms, it is easy to integrate various sensors in IoT devices. Due to the fact that most IoT devices' design are proprietary, it is critical to enumerate all the sensors that are used by an IoT device, especially given the privacy aspect of the data these sensors might collect. The list of factors within this category is shown below.

- *Audio:* whether the device has audio capturing capabilities;
- *Video:* whether the device is equipped with a camera;
- *Motion:* whether the device embeds a motion sensor;
- *Location:* whether the device has geolocation capabilities;
- *Environment:* whether the device captures any other aspect of its environment, such as the temperature, humidity level, etc.

Connectivity (Information). IoT devices can be classified in two basic categories [5]. One category, which includes TV set-top boxes, uses already-existing networking technologies such as Wi-Fi and Ethernet connections.

The other category, which includes sensors, may use different wireless technologies that better suit some of the devices' needs, such as lower energy consumption or ad-hoc network coverage. The list of factors within this category is shown below.

- Ethernet/LAN
- Wi-Fi
- Bluetooth
- ZigBee
- Z-Wave

3.2 Visual Layouts

Two visual layouts are proposed in this section. The first candidate (Fig. 1) is close to the design of the FAD nutrition facts label using a similar design strategy to convey aforementioned device factors to the consumers. We use the common knowledge color system - red and yellow - to highlight severe and cautious security and privacy factors. The second candidate (Fig. 2) leverages icons with text to convey high-level information to the consumers. This design is motivated by the fact that considerable consumers have smartphones and may be responsive to icons. Similarly we use the same color system to highlight security and privacy factors. Note that we leave the user study of these two visual layouts as part of future work.

3.3 Implementation

Extracting information from IoT devices to populate or verify already populated device factors can be achieved using essentially three different techniques: (i) passive discovery, (ii) active probing (fuzzing) and (iii) hardware and software analysis.

Passive discovery techniques consists in deploying the device in a realistic smart home environment testbed and observing the behavior resulting from a normal use of the device. This way we can uncover various communication-related aspects of the device, such as the network protocols it uses, whether the traffic is encrypted or what kind of data is exchanged between the device and the Internet. Existing tools, such as Wireshark [4] and the Nessus Network Monitor [23] are commonly used to passively extract intelligence from network traffic [9]. Some research has also been performed to extract intelligence from passive network communication monitoring, for instance by analyzing patterns in network traffic [11]. However, passive discovery cannot explore all possible behaviors an IoT device can possibly exhibit. Moreover, it provides limited information for IoT devices that generate few or no network traffic or when network communications are encrypted.

Alternatively, *active probing (or fuzzing)* consists in actively testing the device against different inputs in order to trigger as many behaviors as possible. This approach is thus complementary to the passive discovery one. Some existing tools, such the Nessus Scanner [3] or OpenVAS [2] are available and

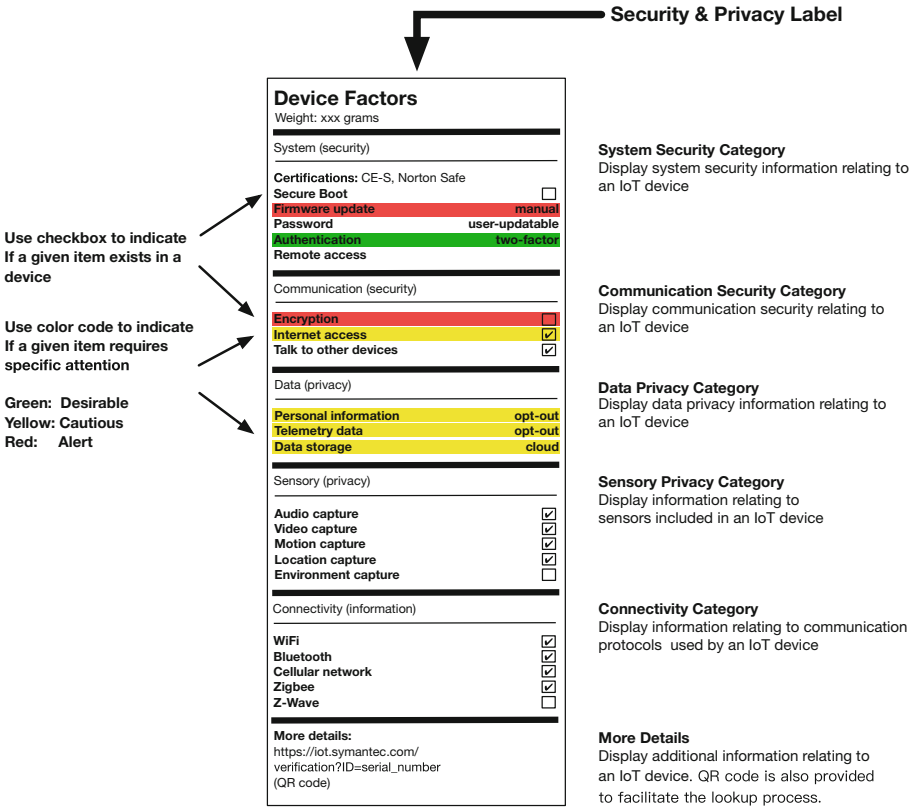


Fig. 1. Candidate visual layout 1: leverage the design concepts of food nutrition facts.

the research community has also been working on IoT-specific fuzzing techniques [14]. However, the peculiarities of IoT devices, for instance the over-presence of sensors [22], tend to significantly increase the attack surface to analyze and usually require fuzzing techniques to be adapted for the assessment of IoT devices.

Finally, *hardware and software analysis* techniques help uncover lower-level characteristics of IoT device systems that can hardly by observed otherwise. For instance, the presence of some sensors, such as a GPS chip, can only be found by inspecting the firmware or even the hardware of a device. Determining whether user data stored on the device is properly handled and is not transmitted back to the manufacturer without the user consent may also require a thorough review of the device firmware. Techniques such as static and dynamic analysis of device firmware, reverse engineering of embedded applications and automated code review are often used in this scenario. While research to uncover vulnerabilities in IoT device firmware [13,15,16,25] or privacy data leaks [12] has already been carried out in this area, some problems remain to be solved and require further research. Moreover, this task is more challenging in the IoT world due to the heterogeneity of IoT device hardware architectures and operating systems.

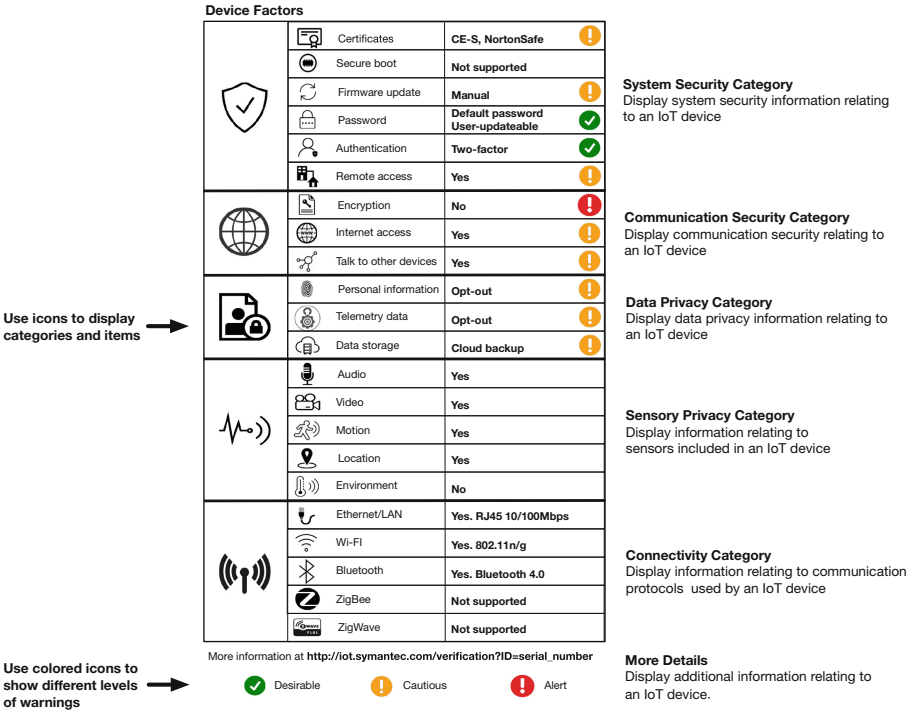
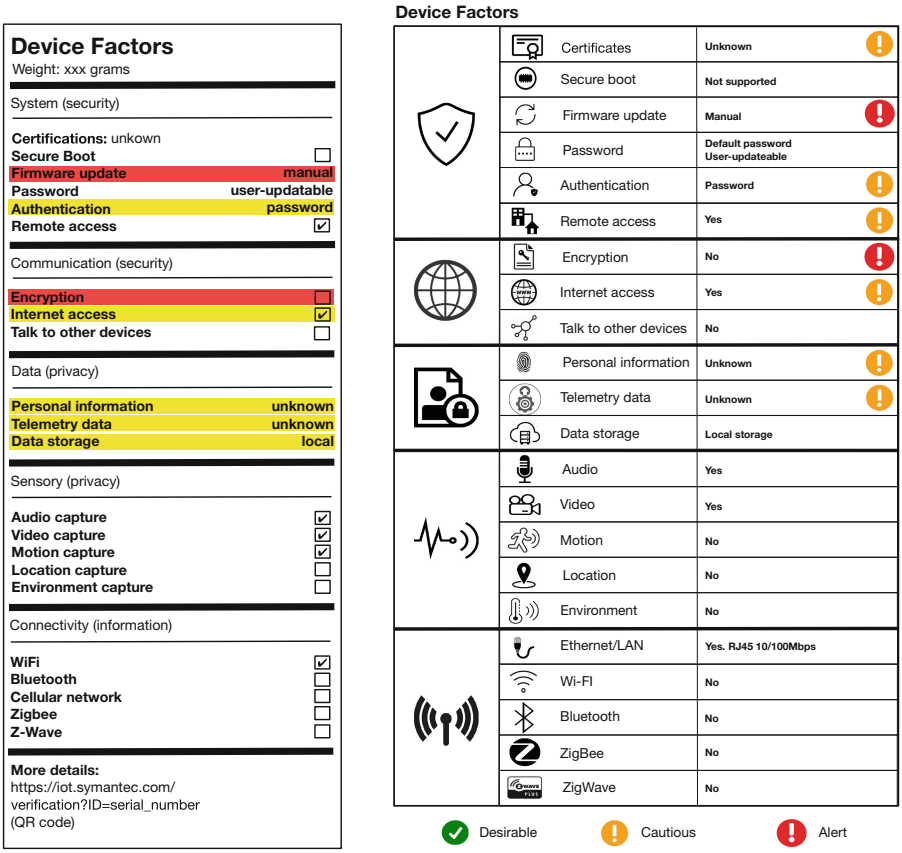


Fig. 2. Candidate visual layout 2: leverage icons and text.

4 Case Study - TVT DVR

TVT Digital Technology Co., Ltd is the manufacturer of over 70 white-labelled Digital Video Recorders (DVRs) for different companies. Its DVR series was found to be [6] and remains as of today [8] vulnerable to attacks from the Mirai botnet and its variants (e.g., Tsunami) according to the latest research. Several factors contributed to its poor security posture. First of all, the TVT DVR series doesn't enforce encrypted communication allowing the attackers to eavesdrop on video feeds (i.e., privacy leakage) and steal login credentials (i.e., security breach). Secondly, it doesn't enforce password change during the setup process even though the users can update the password afterwards. More importantly, it doesn't support over-the-air (OTA) firmware update. The customers have to update the firmware manually. This manual update process is not scalable nor automated, hence the manufacturers cannot roll out critical patches to the customers in a timely manner. Finally the manufacturer doesn't provide clear information on potential private and telemetry data collection.

How can our proposed IoT security and privacy labels help in this particular case? We demonstrate our labels in Fig. 3a and b. These two candidates are able to capture and flag several severe security and privacy problems - unencrypted communication and manual firmware update. These fields are accord-



(a) Candidate layout 1. (b) Candidate layout 2.

Fig. 3. Device factors: TVT DVR. (Color figure online)

ingly highlighted in red. These labels also notify the potential consumers that there are some undesirable factors highlighted in yellow/amber, e.g., password-based authentication and remote access from the Internet is enabled, the data collection procedure is not disclosed, certificates coming with the system are not disclosed, etc.

5 Discussion

In Sect. 3, we presented the IoT factors designed to help consumers in their purchasing of IoT devices. We described the different factors devices should be evaluated against and we elaborated on the implementation of the whole system. In this Section we further discuss some challenges faced in the design, implementation, maintenance and adoption of the IoT device factors.

The device factors presented in Sect. 3.1 constitute a tradeoff between providing an as thorough as possible security and privacy posture of an IoT device and providing a high-level enough summary of this posture. However, IoT security and privacy factors would ideally provide different levels of technical details so consumers with different levels of expertise would find the relevant information they need.

Additionally, we focused on designing device factors that are persistent and have a long validity period. That means that factors shall not change over the course of the device lifetime. However, given the rapidly evolving IoT threat landscape [24] IoT devices should be updated frequently to maintain the highest level of security. Such updates to the devices firmware are likely to change their posture with respect to the security and privacy factors. This introduces the challenge of updating IoT factors. Consequently, a single IoT device could have a different security and privacy posture over time depending on the release of software updates that would fix previously uncovered issues. This could have a cascading effect in the event IoT factors would be printed on the device packages; multiple packages for the same device potentially exhibiting different factors depending on when they were manufactured. A solution to that problem would be to provide additional information through an online service thus ensuring always up-to-date data.

Here above we discussed the motivation behind defining long-lived or "static" device factors. However, as we have seen, these factors are limited to capture "static" aspects of IoT devices. Extending this model to dynamic factors – which would likely vary much more across time and depending on a device usage and environment – would enable a more thorough and fine-grained security and privacy assessment of the device. For instance, software vulnerabilities are regularly uncovered in IoT device firmware, which turns out to be the main attack vector to infect and compromise IoT devices. Such vulnerabilities can include faulty applications, weak authentication mechanisms, use of outdated or broken encryption algorithms, etc. These vulnerabilities then need to be fixed through software updates, which is handled more or less diligently by the different manufacturers. Including such a software vulnerability assessment in the factors would thus provide a very informative assessment of a device's security posture.

Recently, the European Union Agency for Network and Information Security (ENISA) published a report [17] on best practices for the development and deployment of IoT devices. While these guidelines are seldom followed in practice, they should be reflected in the factors and used to evaluate the security and privacy posture of IoT devices. One feasible strategy is making ENISA best practices enforceable. All IoT devices must be certificated following its guidance through a rigorous procedure. In this way, the manufacturers are responsible to produce factual security and privacy labels. In turn, these labels produced by the IoT device manufacturers can be verified and tested by third party watchdogs and hold them accountable if any violations are identified.

Finally, one of the reasons why IoT devices are riddled with vulnerabilities and design flaws is the pressure manufacturers have to flood the market with

new devices providing an ever growing set of functionalities. This aggressive development often comes at the price of poorly manufactured devices. We believe that the introduction of IoT labels is likely to motivate manufacturers to improve their products in order to keep them competitive.

6 Conclusion

In response to the increasing number of attacks against IoT devices and the rampant poorly manufactured devices that offer poor or no protection to their users, we propose IoT security and privacy fact labels. These labels aim at offering consumers a high-level assessment of the security and privacy posture of IoT devices to help in the buying process. We introduce a classification of IoT device factors that we believe offer a good tradeoff between simplicity and completeness. We also provide two possible layouts for a quick and easy visualization of a device security and privacy posture. Finally, we elaborate on the challenges to be faced to implement these IoT device factors. Indeed, while the information provided in the device factors is summarized and high-level, populating these factors requires further research to perform in-depth profiling and exploration of IoT devices hardware and software.

References

1. Mirai: what you need to know about the botnet behind recent major DDoS attacks. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks
2. OpenVAS - Open Vulnerability Assessment System. http://openvas.org/
3. The Nessus Scanner. https://www.tenable.com/products/nessus/nessus-professional
4. Wireshark. https://www.wireshark.org/
5. Insecurity in the Internet of Things (2015). https://www.symantec.com/content/en/us/enterprise/iot/b-insecurity-in-the-internet-of-things_21349619.pdf
6. Remote Code Execution in CCTV-DVR affecting over 70 different vendors (2016). http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html
7. "BrickerBot" Results In PDoS Attack (2017). https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/
8. New IoT/Linux Malware Targets DVRs, Forms Botnet (2017). http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
9. Alrawi, O., Lever, C., Antonakakis, M., Monrose, F.: SoK: security evaluation of home-based IoT deployments. In: IEEE S&P (2019)
10. Antonakakis, M., et al.: Understanding the mirai botnet. In: USENIX Security (2017)
11. Apthorpe, N., Reisman, D., Feamster, N.: A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic. In: DAT (2017)
12. Celik, Z.B., et al.: Sensitive information tracking in commodity IoT. In: USENIX Security (2018)

13. Chen, D.D., Woo, M., Brumley, D., Egele, M.: Towards automated dynamic analysis for Linux-based embedded firmware. In: NDSS (2016)
14. Chen, J., et al.: IoTFuzzer: discovering memory corruptions in IoT through app-based fuzzing. In: NDSS (2018)
15. Costin, A., Zaddach, J., Francillon, A., Balzarotti, D.: A large scale analysis of the security of embedded firmwares. In: USENIX Security (2014)
16. Costin, A., Zarras, A., Francillon, A.: Automated dynamic firmware analysis at scale: a case study on embedded web interfaces. In: ASIACCS (2016)
17. ENISA. Baseline Security Recommendations for IoT (2017). https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
18. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A nutrition label for privacy. In: USENIX SOUPS (2009)
19. Kelley, P.G., Cesca, L., Bresee, J., Cranor, L.F.: Standardizing privacy notices: an online study of the nutrition label approach. In: CHI (2010)
20. Naeini, P.E., Agarwal, Y., Cranor, L., Dixon, H.: Exploring how privacy and security factor into IoT device purchase behavior. In: USENIX SOUPS (2017)
21. Naeini, P.E., et al.: Privacy expectations and preferences in an IoT world. In: USENIX SOUPS (2017)
22. Sikder, A.K., Petracca, G., Aksu, H., Jaeger, T., Uluagac, A.S.: A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications (2018). https://arxiv.org/pdf/1802.02041.pdf
23. Tenable: Nessus Network Monitor (2018). https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/Tenable2018_DS-Nessus-Network-Monitor.pdf
24. Pierre-Antoine, V., Shen, Y.: Before toasters rise up: a view into the emerging IoT threat landscape. In: RAID (2018)
25. Zaddach, J., Bruno, L., Francillon, A., Balzarotti, D.: Avatar: a framework to support dynamic security analysis of embedded systems' firmwares. In: NDSS (2014)