Opinion: Security Lifetime Labels – Overcoming Information Asymmetry in Security of IoT Consumer Products

Philipp Morgner
Friedrich-Alexander-Universität
Erlangen-Nürnberg
philipp.morgner@fau.de

Felix Freiling
Friedrich-Alexander-Universität
Erlangen-Nürnberg
felix.freiling@fau.de

Zinaida Benenson
Friedrich-Alexander-Universität
Erlangen-Nürnberg
zinaida.benenson@fau.de

ABSTRACT

The installed base of Internet of Things (IoT) consumer products is steadily increasing, in conjunction with the number of disclosed security vulnerabilities in these devices. In this paper, we share the opinion that strong security measures are necessary but IoT security cannot solely be improved by means of sophisticated technical solutions. From our point of view, economic incentives for the manufacturers have to be established through enabling consumers to reward security. This is currently not the case, as an asymmetric information barrier prevents consumers from assessing the level of security that is provided by IoT products. As a result, consumers are not willing to pay for a comprehensive security design as they cannot distinguish it from insufficient security measures. Learning from regulatory approaches that overcame information asymmetries about other non-functional properties in consumer products, e.g., energy labels to compare the power consumption, we propose *security lifetime labels*, a mechanism that transforms security into an accessible feature and enables consumers to make informed buying decisions. Focusing on the delivering of security updates as an important aspect of enforcing IoT security, we aim to transform the asymmetric information about the manufacturers' willingness to provide security updates into a label that can be assessed by the consumers.

CCS CONCEPTS

• **Security and privacy → Economics of security and privacy**; *Distributed systems security*;

KEYWORDS

IoT, security, updates, labels, economics, information asymmetry

1 INTRODUCTION

The Internet of Things (IoT) promises to enhance our lives in several ways: it improves life quality, increases energy efficiency, and automates workflows. According to an estimation [16], 7 billion IoT consumer devices will be installed at the end of 2018. Furthermore, the prediction says that the global market of IoT consumer products achieves a revenue of 1.5 trillion US Dollars in 2020. Thus, a lot of business stakeholders release products to gain a share of this market.

This development leads to the critical situation where products are released to the market with some kind of security measures – but as the current discussion about IoT security shows, these mechanisms are not comprehensive enough. Recently disclosed security issues in IoT consumer products range from unsecured data transmissions [28, 36], leaked master keys [46], and unsecured backends [5, 7, 17] to insufficient physical security mechanisms [28], overprivileged applications [13, 17], hard-coded credentials [7], and implementation bugs [19, 31, 34]. A lot of technical solutions and frameworks have been proposed [6, 14, 21, 26, 39, 43] that could improve the security of IoT consumer products today. However, we expect that the spillover of academic security research into real-world IoT products is going to be slow or will not happen at all, as we have experienced in the past.

We believe that further research in technical security solutions alone will not lead to substantial improvements in the security of IoT consumer products. In fact, IoT security can only be enhanced by considering the business goals of the manufacturers and creating economic incentives for applying stronger security measures. From our point of view, an asymmetric information barrier exists as consumers are not able to determine the level of security that is provided by an IoT consumer product. Even manufacturers might not be aware about their products' level of security [18]. As a consequence, consumers do not reward security, and thus, manufacturers do not invest in such measures. To overcome this unfortunate situation, we discuss the idea of a mechanism that makes security, especially in terms of updates provided by the manufacturer, assessable for consumers. For the realization, legislation is required, which demands a *security lifetime label* for each product that is newly released to the market. Our proposal learns from the examples of other labels that have been introduced to overcome information asymmetries, e.g., energy consumption labels that inform the consumer about the energy efficiency or operating costs of electronic consumer products. The same way these labels reduced information asymmetries, the proposed security lifetime label transfers the manufacturer's willingness of providing security updates for a certain period of time into an assessable and comparable feature allowing consumers to make informed buying decisions that also consider security properties.

2 CONSUMERS CANNOT ASSESS SECURITY

Manufacturers are not rewarded for making products secure since the consumers are not able to assess the level of security provided by an IoT product [3, 4]. As established in the economic theory of the 'market for lemons' [1], consumers are not willing to pay for something they cannot measure. This applies especially to security:

WiSec '18, June 18–20, 2018, Stockholm, Sweden

ACM ISBN 978-1-4503-5731-9/18/06…$15.00
https://doi.org/10.1145/3212480.3212486

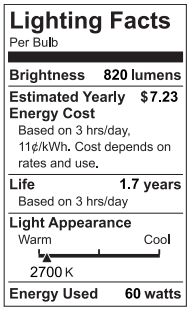
how can a consumer determine the level of security that is provided by a product? Even if a product claims to be highly secure and uses the strongest encryption schemes, a non-expert user cannot determine if this is reasonable [27]. Consumers reward manufacturers for providing an attractive and feature-rich product and being the first on the market. As resources for developing a new product are finite, functional features are prioritized over non-functional features, such as a comprehensive security and update architecture. Thus, in the first phase of an evolving technology, manufacturers focus on functional features, quick time-to-market, and neglect security. Strong security features are added in a later phase, when the product has achieved a solid market position [3]. Thus, the goal of our approach is a paradigm shift in which security becomes a feature that can be assessed and compared by the consumers.

3 CONSUMER PRODUCT LABELING

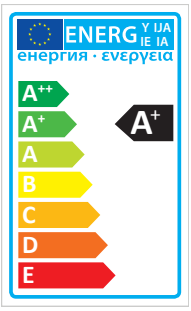
In many countries, legislation exists that demands consumer products to be tagged with certain labels and marks. Marks are symbols that range from indicating danger to the proper recycling of the product, whereas labels indicate more specific information about the product in form of written text, scales, or numerical statements. While most marks and labels are mandatory, there also exists a number of voluntary signs that are mainly used as marketing tools. In the USA, the Federal Trade Commission (FTC) is responsible for labeling policies. In the EU, each member state has its own institution that executes legislation and regulations defined by the EU Commission. In the following, we present three examples of mandatory labels that have been introduced in order to reduce information asymmetries.

The FTC introduced the Energy Labeling Rule [11] as part of the Energy Independence and Security Act of 2007 [23], which makes it mandatory to mark a number of consumer products, e.g., dishwashers, televisions, and other appliances, with a label as depicted in Figure 1a. These labels show the energy consumption as well as the estimated annual operating costs compared to the range of operating costs for product of the same category. Also, the EU introduced an energy label with the Energy Efficiency Directive [10] in 2010. The label indicates the energy efficiency for a wide range of products by categorizing the power consumption of this product. An example is shown in Figure 1b. The overall objective of this label is to incentivize manufacturers to design more energy-efficient products aiming for the reduction of the overall energy consumption of the EU by 20% until 2020 [8]. The third example is the EU Tire Label introduced with the Directive EC/1222/2009 [9] in November 2009. This label informs consumers about the fuel efficiency, wet grip performance, and rolling noise of tires for passenger cars as well as light and heavy duty vehicles. The goal is to allow consumers to make informed buying decisions considering safety, environmental and economic efficiency along with other properties that are usually considered during buying decisions.

From an economic perspective, when consumers make buying decisions, it involves the risk of suffering some kind of loss [35]. To reduce the risk of loss for the consumers, already a wide range of mechanisms exist, so-called risk relievers. Examples of such risk relievers are warranty, endorsements by friends and experts, brand image, money-back guarantee, private or governmental testing, among others. The perception of risk plays an important role in



(a) FTC Energy Label



(b) EU Energy Label

Figure 1: Examples of mandatory product labels

the buying decision. Hence, the manufacturer has to decide on a trade-off between the economic costs of providing a risk reliever and the hopefully increasing profits from larger sales generated by reducing the consumers' hesitation [35]. In this context, a label fulfills two main functions: it informs the user about intangible product attributes (information function) and holds a value itself as a value function, e.g., prestige. Furthermore, it guides consumers to compare product with each other to make an informed buying decision. Studies on the influence of energy efficiency labels [37, 42, 44] conclude that consumers are aware of these labels and understand them. Also, consumers state that these labels influence their buying decisions [37].

To advance our objective of removing the asymmetric information barrier regarding the security of IoT consumer products, we propose a mandatory label that shows security-related information to guide consumers in making informed buying decisions.

4 SECURITY AS A COMPARABLE FEATURE

What kind of information (potentially printed as a label on the product) is suitable to indicate the level of security that is provided by an IoT consumer product? In our opinion, the listing of applied cryptographic schemes and certification programs is not suitable since they are not understandable for non-expert users. A product's certification might imply that the whole product is certified, while in reality only a subset of the components underwent a certification process [29]. Moreover, technically certified frameworks might even be insecure as a result of a flawed implementation. Our approach is based on the hypothesis that patching security flaws in IoT products is more crucial than the insecurities themselves. Insufficient security designs and implementation bugs will always be around. Studies investigated the number of vulnerabilities in software and stated that the average number of defects in well-engineered software lies at around 2 defects per 1000 lines of code [2, 24]. As human beings, we create imperfect code such that the primary objective of security has to be the patching of software as soon as defects are disclosed.

Previous studies on security patching [15, 22, 38] conclude that most vulnerabilities are fixed prior or at the day of their public disclosure (assuming that the vendor was informed before going public), while others take up to a few months after disclosure. In some cases, vendors even refuse to deliver patches. Their reasons might be a lack of experience or missing economic incentives for fixing their products in a timely manner.

5 SECURITY LIFETIME LABELS

From our point of view, incentives for the timely delivering of software updates can be established by legislation that demands a mandatory *security lifetime label* for all newly released IoT consumer products, based on an *update policy*. The update policy is set by the brand-giving company and states the following information:

- **Security Lifetime:** The security lifetime of a product determines the timeframe in which the manufacturer ensures the patching of security vulnerabilities in the product's software. In other words, it defines for how long the manufacturer contractually warrants to provide security updates. The security lifetime has to be absolute since the consumer usually does not know the production date of the device. Also, it would not be in the interest of a company to provide updates for a relative period of time based on the selling date of a product since there can be years between the production and the selling of a product.
- **Time to Patch:** When a security vulnerability in the software was reported, the manufacturer has to investigate this issue and patch the software if needed. The update policy should define within which maximum timeframe the manufacturer guarantees to provide software security patches.

The proposed legislation to execute this update policy defines only the obligations between buyers and the brand-giving company of the purchased IoT consumer product, while the interactions between the brand-giving company and original equipment manufacturers (or other third parties) should be regulated by the market itself.

In this sense, a security lifetime label might act similarly to a warranty. From the perspective of the manufacturers, warranty protects them from unjustified claims [40] and has the function as a marketing variable [20]. For consumers, warranty can act as a risk reliever [33], and increases the trust in product quality and value [12, 30].

The proposed legislation determines that each product has a mandatory label that transforms the experience characteristic 'lifetime support' into a search attribute, i.e., showing the absolute lifetime (e.g., 'Supported until 11/2026') and the time to patch (e.g., 'Time to patch: less than 3 months'). This label is printed on the product itself as well as on the packaging of the product such that the consumers can consider these facts as they make a buying decision. If a product does not support this policy, it gets a 'Zero lifetime' and 'No patches' label. This might be the case for non-updatable products or if the manufacturer intentionally refuses to provide updates.

As soon as a suspected vulnerability is found, the finder needs a way to report this issue. While this is usually done by informing an appropriate security incident response team via email, this informal way lacks documentation for the legislation enforcing institutions. Thus, another way has to be implemented that provides a trusted documentation for all concerning parties. The scope of the proposed legislation should also consider these mechanisms.

In case the manufacturer is not able to act according to its update policy, i.e., the vendor cannot fix the security vulnerability within the self-defined period of time, then the consumer should be able to claim compensation. If the manufacturer is able to patch the security flaws within the self-defined period of time, then the consumers cannot claim compensations for the security flaws since they made an informed decision when buying these products.

6 DISCUSSION

There exist a number of legitimate issues concerning the effectiveness and user acceptance of security lifetime lables. Below we briefly discuss some of these concerns.

Prior research [41] showed that consumers are often reluctant to install updates. This reluctance originates from negative update experiences in the past and is mostly associated with unwanted changes in the user experience like the remodeling of user interfaces. These negative experiences of functional updates could also affect the installation of security updates, as most users do not distinguish between different types of updates.

Another concern is that security lifetime labels could create a false sense of security. Consumers might believe that the security of a product is guaranteed at all times until the end of the security lifetime. Thus, the label should be self-explaining and clearly communicate that it does not guarantee security but specifies for how long the manufacturer supports a product with security updates.

Also, moral hazard [32] might be a concern: If a vulnerability does not hurt the owner, why should one pay for a more secure product? A prominent example are the attacks of the Mirai botnet [5] on Internet infrastructure, made possible through insecure IoT consumer devices. Although recent studies on IoT products conclude that security is a major concern for consumers [25, 45], many users do not care about configuring their devices securely as long as they are not directly affected by their products' insecurities.

The circumvention of the proposed legislation by corporations through passing the liability along to brand-giving offshore companies is another legitimate concern. Leaving the definition of a legislation to the legal community, this legislation must of course consider potential loopholes. On the other hand, manufacturers are not forced and can freely decide whether they guarantee future security updates. Instead of tricking (and betraying) the consumers, companies might cover potential financial damages for failing update policies by insurances.

Finally, fundamental flaws in the security architecture might be impossible to fix with software updates, and thus, security lifetime labels will be of no help in such cases. We argue that even in these cases, the threat can usually be contained to a certain level. Moreover, if a labeled product remains insecure after updates, the consumers will be able to demand compensation, which is hardly possible today. Our proposal strengthens consumer protection and motivates manufacturers to put more focus on a comprehensive security strategy.

7 CONCLUSION AND FUTURE WORK

In this paper, we discussed our opinion that IoT security will not solely be improved with technical security measures. Instead, we need a paradigm shift that fosters economic incentives for comprehensive security strategies. As a concrete idea, we propose a legislation for security lifetime labels, which overcomes the information asymmetry between consumers and manufacturers about the manufacturers' willingness to provide security updates.

Future work should empirically investigate the impact of the proposed security lifetime label on the buying decisions of consumers. In addition, vulnerability response procedures as well as effective sanctioning have to be designed and evaluated.

ACKNOWLEDGMENTS

This work is supported by the German Research Foundation (DFG) under Grant BE 5440/2-1. We thank the anonymous reviewers for helpful comments, and the participants of the Dagstuhl Seminar 16461 for the initial discussions about issues with unpatched IoT devices.

REFERENCES

[1] George A. Akerlof. 1970. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics* 84, 3 (1970), 488–500.

[2] Omar H. Alhazmi, Yashwant K. Malaiya, and Indrajit Ray. 2007. Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers & Security* 26, 3 (2007), 219–228. https://doi.org/10.1016/j.cose.2006.10.002

[3] Ross Anderson. 2001. Why Information Security is Hard-An Economic Perspective. In *17th Annual Computer Security Applications Conference (ACSAC 2001)*.

[4] Ross Anderson and Tyler Moore. 2006. The Economics of Information Security. *Science* 314, 5799 (2006), 610–613.

[5] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the Mirai Botnet. In *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*. 1093–1110.

[6] Imane Bouij-Pasquier, Anas Abou El Kalam, Abdellah Ait Ouahman, and Mina De Montfort. 2015. A Security Framework for Internet of Things. In *Cryptology and Network Security - 14th International Conference, CANS 2015, Marrakesh, Morocco, December 10-12, 2015, Proceedings*. 19–31.

[7] Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. 2014. A Large-Scale Analysis of the Security of Embedded Firmwares. In *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014*. 95–110.

[8] European Commission. 2017. Energy Efficiency Directive. https://ec.europa.eu/energy/en/topics/energy-efficiency/energy-efficiency-directive

[9] European Parliament and the Council of the European Union. 2009. Regulation (EC) No 1222/2009. *Official Journal of the European Union*. http://eur-lex.europa.eu/legal-content/EN/ALL/?uriCELEX:32009R1222

[10] European Parliament and the Council of the European Union. 2010. Directive 2010/30/EU. *Official Journal of the European Union*. http://eur-lex.europa.eu/legal-content/EN/ALL/?uriCELEX:32010L0030

[11] Federal Trade Commission. 2018. Energy and Water Use Labeling for Consumer Products Under the Energy Policy and Conservation Act ("Energy Labeling Rule"). https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/energy-water-use-labeling-consumer

[12] Laurence P. Feldman. 1976. New Legislation and the Prospects for Real Warranty Reform. *Journal of Marketing* 40, 3 (1976), 41–47. http://www.jstor.org/stable/1249993

[13] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security Analysis of Emerging Smart Home Applications. In *IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016*. 636–654.

[14] Earlence Fernandes, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti, and Atul Prakash. 2016. FlowFence: Practical Data Protection for Emerging IoT Application Frameworks. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*. 531–548.

[15] Stefan Frei, Martin May, Ulrich Fiedler, and Bernhard Plattner. 2006. Large-Scale Vulnerability Analysis. In *Proceedings of the 2006 SIGCOMM Workshop on Large-Scale Attack Defense*. ACM, 131–138.

[16] Gartner. 2017. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. https://www.gartner.com/newsroom/id/3598917

[17] Dan Goodin. 2015. 9 Baby Monitors Wide Open to Hacks that Expose Users' Most Private Moments. *Ars Technica* (September 2015). https://arstechnica.com/information-technology/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/

[18] Ian Grigg. 2008. The Market for Silver Bullets.

[19] Alex Hern. 2016. Someone Made a Smart Vibrator, so of Course It Got Hacked. *The Guardian* (August 2016). https://www.theguardian.com/technology/2016/aug/10/vibrator-phone-app-we-vibe-4-plus-bluetooth-hack

[20] C. L. Kendall and Frederick A. Russ. 1975. Warranty and Complaint Policies: An Opportunity for Marketing Management. *Journal of Marketing* 39, 2 (1975), 36–43. http://www.jstor.org/stable/1250113

[21] Jun Young Kim, Wen Hu, Dilip Sarkar, and Sanjay Jha. 2017. ESIoT: Enabling Secure Management of the Internet of Things. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2017, Boston, MA, USA, July 18-20, 2017*. 219–229.

[22] Frank Li and Vern Paxson. 2017. A Large-Scale Empirical Study of Security Patches. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. 2201–2215.

[23] Library of Congress. 2007. H.R.6 - Energy Independence and Security Act of 2007. https://www.congress.gov/bill/110th-congress/house-bill/6

[24] Yashwant K. Malaiya and Jason Denton. 1998. Estimating the Number of Residual Defects. In *3rd IEEE International Symposium on High-Assurance Systems Engineering (HASE '98), 13-14 November 1998, Washington, D.C, USA, Proceedings*. IEEE Computer Society, 98–107. https://doi.org/10.1109/HASE.1998.731600

[25] McAfee. 2018. New Security Priorities in An Increasingly Connected World. https://securingtomorrow.mcafee.com/consumer/key-findings-from-our-survey-on-identity-theft-family-safety-and-home-network-security/

[26] Mujahid Mohsin, Zahid Anwar, Farhat Zaman, and Ehab Al-Shaer. 2017. IoTChecker: A Data-Driven Framework for Security Analytics of Internet of Things Configurations. *Computers & Security* 70 (2017), 199–223.

[27] Philipp Morgner and Zinaida Benenson. 2018. Exploring Security Economics in IoT Standardization Efforts. *Proceedings of the NDSS Workshop on Decentralized IoT Security and Standards, DISS'18, San Diego, CA, USA, February 18, 2018*.

[28] Philipp Morgner, Stephan Mattejat, Zinaida Benenson, Christian Müller, and Frederik Armknecht. 2017. Insecure to the Touch: Attacking ZigBee 3.0 via Touchlink Commissioning. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2017, Boston, MA, USA, July 18-20, 2017*. 230–240.

[29] Steven J. Murdoch, Mike Bond, and Ross Anderson. 2012. How Certification Systems Fail: Lessons from the Ware Report. *IEEE Security & Privacy* 10, 6 (2012), 40–44. https://doi.org/10.1109/MSP.2012.89

[30] Jerry C Olson and Jacob Jacoby. 1972. Cue Utilization in the Quality Perception Process. *ACR Special Volumes* (1972).

[31] Danny Palmer. 2017. Security Flaw in LG IoT Software Left Home Appliances Vulnerable. *ZDNet* (October 2017). http://www.zdnet.com/article/security-flaw-in-lg-iot-software-left-home-appliances-vulnerable/

[32] Mark V. Pauly. 1968. The Economics of Moral Hazard: Comment. *The American Economic Review* 58, 3 (1968), 531–537. http://www.jstor.org/stable/1813785

[33] Michael Perry and Arnon Perry. 1976. Service Contract Compared to Warranty as a Means to Reduce Consumer's Risk. *Journal of Retailing* 52, 2 (1976), 33 – 90.

[34] Eyal Ronen, Colin O'Flynn, Adi Shamir, and Achi-Or Weingarten. 2017. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*. 195–212.

[35] Ted Roselius. 1971. Consumer Rankings of Risk Reduction Methods. *Journal of Marketing* 35, 1 (1971), 56–61. http://www.jstor.org/stable/1250565

[36] Mike Ryan. 2013. Bluetooth: With Low Energy Comes Low Security. In *7th USENIX Workshop on Offensive Technologies, WOOT '13, Washington, D.C., USA, August 13, 2013*.

[37] Katharina Sammer and Rolf Wüstenhagen. 2006. The Influence of Eco-Labelling on Consumer Behaviour – Results of a Discrete Choice Analysis for Washing Machines. *Business Strategy and the Environment* 15, 3 (2006), 185–199. https://doi.org/10.1002/bse.522

[38] Muhammad Shahzad, Muhammad Zubair Shafiq, and Alex X. Liu. 2012. A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles. In *34th International Conference on Software Engineering, ICSE 2012, June 2-9, 2012, Zurich, Switzerland*. 771–781.

[39] Vishal Sharma, Kyungroul Lee, Soonhyun Kwon, Jiyoon Kim, Hyungjoon Park, Kangbin Yim, and Sun-Young Lee. 2017. A Consensus Framework for Reliability and Mitigation of Zero-Day Attacks in IoT. *Security and Communication Networks* 2017 (2017), 4749085:1–4749085:24. https://doi.org/10.1155/2017/4749085

[40] Jon G. Udell and Evan E. Anderson. 1968. The Product Warranty as an Element of Competitive Strategy. *Journal of Marketing* 32, 4 (1968), 1–8.

[41] Kami Vaniea, Emilee J. Rader, and Rick Wash. 2014. Betrayed by Updates: How Negative Experiences Affect Future Security. In *CHI Conference on Human Factors in Computing Systems, CHI'14, Toronto, ON, Canada - April 26 - May 01, 2014*. 2671–2674.

[42] Paul Waide. 2001. Monitoring of Energy Efficiency Trends of Refrigerators, Freezers, Washing Machines and Washer-Driers Sold in the EU, Final Report. *PW Consulting for ADEME on behalf of the European Commission (SAVE). PW Consulting: Manchester* (2001).

[43] Qi Wang, Wajih Ul Hassan, Adam Bates, and Carl Gunter. 2018. Fear and Logging in the Internet of Things. In *Network and Distributed Systems Symposium, NDSS'18, San Diego, CA, USA, February 19-21, 2018*.

[44] John Winward, Pernille Schiellerup, and Brenda Boardman. 1998. *Cool Labels: The First Three Years of the European Energy Label*. Energy and Environment Programme, Environmental Change Unit, Univ. of Oxford.

[45] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security, SOUPS 2017, Santa Clara, CA, USA, July 12-14, 2017*. 65–80.

[46] Tobias Zillner and Sebastian Strobl. 2015. ZigBee exploited – The Good, the Bad and the Ugly. (2015). https://www.blackhat.com/us-15/briefings.html#zigbee-exploited-the-good-the-bad-and-the-ugly Black Hat USA.