Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software: NIST Submission

Prof Shane Johnson[1] and Dr John Blythe[1]
[1] Dawes Centre for Future Crime at University College London

Over the period 2017 to 2019, we conducted a series of studies to assess the potential utility of consumer labelling schemes to improve the security of the Internet of Things. The research was part of the UK's PETRAS National Centre of Excellence for IoT Systems Cybersecurity and conducted in collaboration with the Department of Dgitial, Culture, Media and Sport within UK Government - the department tasked with securing consumer IoT.The general lessons learned from this work are likely to also inform the challenges associated with, and practical approaches to, consumer software labelling and hence we are submitting this document to the NIST call for papers on Cybersecurity Labelling for Consumers.

In our work, we systematically reviewed the literature (academic and media) to identify crimes that have or could plausibly be committed using insecure IoT devices (Blythe and Johnson, 2019; Johnson et al., 2021); conducted market surveillance research to examine what is communicated to consumers before the purchase of devices, and what cyberhygiene advice is provided (Blythe et al., 2019); reviewed the literature on the effect of labelling schemes on other types of products (Blythe and Johnson, 2019); engaged with stakeholders (e.g. industry, government, law enforcement) about the challenges (and potential solutions) to developing a security labelling scheme for the IoT; conducted surveys and experiments with consumers to explore what matters most to them, the impact that labels might have on their purchasing decisions, and what they would be willing to pay for increased security for different types of consumer IoT devices (Blythe et al., 2019; Johnson et al., 2020).

In Blythe et al. (2019) we compiled a database of 270 consumer IoT devices produced by 220 different manufacturers on sale at the time of the study. The security features identified were then mapped to the UK Government's Secure by Design Code of Practice for IoT devices to examine the extent to which devices currently on the market appear to conform to it. The user manuals and associated support pages for these devices were then analysed to provide a 'consumer eye' view of the security features they provide and the cyber hygiene advice that is communicated to users. Our findings suggest that manufacturers provide too little publicly available information about the security features of their devices, which makes market surveillance challenging and provides consumers with little information about the security of devices before their purchase. For example, for none of the devices examined was information provided about the period over which security updates would be provided. For only 20% of devices were Wi-Fi encryption standards discussed, and in only 10% were features designed to protect the privacy of users discussed. We also found that manufacturers were inconsistent about what details they provide and how they reported them creating a further challenge for consumers to assess security. We would reccinend that a similar exercise be conducted for consumer software.

Our rapid evidence assessment of labelling schemes (Blythe and Johnson, 2018) suggested that (e.g. nutrition or energy) labels are generally effective in influencing consumer and/or manufacturer behaviour but that the different types (e.g. seal of approval labels, graded labels) vary in the extent to which they are understood and the impacts they have on consumer behaviour. A number of biases (including the affect heuristic, whereby a consumer's attention is drawn to some but not all of the information they should consider) were also identified that can distort the effects of different types of labels, and backfire effects were identified for labels that have not been sufficiently tested prior to their use. These issues should be attended to when designing security labels that aim to educate and nudge consumers.

To assess the potential influence of security labels on consumer purchasing decisions, in Johnson et al. (2020) we conducted a stated preference discrete choice experiment (supplemented with a qualitative survey) with 3000 participants. Participants were presented with a simulated purchasing decision and asked to indicate which of a set of products they would be most likely to purchase. We varied the descriptions of the products in terms of price, the functionality of the product (e.g. standard or premium features) and whether they had a security label. Across conditions, we also varied the type of label used so that we could see if different designs have different effects. They did. Overall, we find that security labels affected simulated purchasing decisions, with participants being more likely to say they would purchase those for which there was a label and for those that implied better security. A descriptive informational label (similar to the front-of-packaging nutrition labels) appeared to be particularly effective, and was the only form of label that had the same influence on consumer choice as the functionality of the device. Participants choices suggested that they were willing to pay a non-trivial amount for security (see also Blythe et al., 2019). Qualitative responses suggested that participants would use a label to inform purchasing decisions, and that the labels did not generate a false sense of security.

In workshops with stakeholders, we identified a number of issues that apply to the security of the IoT (and would apply to consumer software) but not to other application areas. These included the complexity of measuring "security" and the fact that (unlike calorific content) the level of protection a device (or software) can provide will be dynamic (which might require a dynamic label). The issue of whether devices should be self-certified or independently tested was discussed and there was general agreement that either could be employed (in parallel) as long as the provenance of the certification for any product was made clear. While issues were identified, there was a clear appetite for the use of an IoT labelling scheme and recognition of the benefits it would provide.

REFERENCES

Blythe, J. M., & Johnson, S. D. (2018). Rapid evidence assessment on labelling schemes and implications for consumer IoT security. Department for Digital, Culture, Media and Sport, https://www.gov.uk/government/publications/rapid-evidence-assessment-on-labelling-schemes-for-iot-security.

Blythe, J. M., & Johnson, S. D. (2019). A systematic review of crime facilitated by consumer Internet of Things. *Security Journal*, 34, 97-125. https://link.springer.com/article/10.1057/s41284-019-00211-8

Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?. *Journal of Cybersecurity*, *5*(1), https://academic.oup.com/cybersecurity/article/5/1/tyz005/5519411?searchresult=1.

Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PloS one*, *15*(1). https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800

Johnson, S.D., Blythe, J.M., Kim, E. and Sombatruang, N. (2021). Crime and the Consumer Internet of Things. In M Gill (Ed.) *The Handbook of Security*, forthcoming.