The Role of Product Reviewers in Evaluating Security and Privacy

Wentao Guo, Jason Walter, Michelle L. Mazurek
University of Maryland

***Abstract*—As consumers adopt new Internet-connected devices, apps, and other software, they are often exposed to security and privacy vulnerabilities that they likely do not have time, expertise, or incentive to evaluate themselves. Can professionals and institutions help by evaluating the security and privacy of these products on behalf of consumers? As a first step, we interview product reviewers about their work, specifically whether and how they incorporate security and privacy. To inform our interview design, we conduct content analysis on published product reviews to identify security- or privacy-relevant content.**

I. Introduction and Motivation

Many Internet-connected devices, apps, and other software have significant security and privacy vulnerabilities that have been exploited in the real world [1]–[4]. Emami-Naeini et al. found that owners of connected devices report security and privacy concerns with their current devices and a desire to know more about security and privacy before future purchases, but they also report difficulty in finding useful information [5]. We investigate how product reviewers provide information to consumers, as they already commonly evaluate products on other criteria, such as functionality and reliability, and their reviews are often consulted by consumers deciding what to purchase. Our definition of product reviews includes those published by non-profit organizations (e.g., Consumer Reports), for-profit media companies (e.g., CNET), and YouTube channels (e.g., Linus Tech Tips). Because we are interested in shifting the burden of evaluating security and privacy from ordinary users to professionals, we exclude customer reviews such as those aggregated on Amazon.com.

II. Analyzing the Content of Product Reviews

To inform our interview design, we assembled a preliminary dataset of 71 product reviews, focusing on three categories of connected devices: smart locks, smart thermostats, and smart doorbell cameras. For each category, we devised one search string for list-style reviews and one for single-product reviews; e.g., for thermostats, we used "best smart thermostats review" and "Nest thermostat review." We searched Google, Bing, and YouTube with each string, and we downloaded the top five relevant results. Nineteen results appeared on both Google and Bing, for a total of 41 text reviews and 30 video reviews.

We are analyzing the security- and privacy-related content of these product reviews through qualitative coding. We developed our initial codebook inductively while reading other reviews of various Internet-connected devices, apps, and other software. We also incorporated relevant concepts from the Digital Standard [6], a framework developed to guide the design and evaluation of products along consumer values. Two researchers refined the codebook while collaboratively coding 21 reviews from our dataset; they then coded 9 reviews independently, reaching a Krippendorff's α of 0.83, which indicates good inter-rater reliability [7]. All remaining reviews requiring coding or recoding have been divided between the two researchers.

Our analysis compares different review styles, as well as different product categories. We focus on two main research questions:

1) What information relevant to security and privacy do these product reviews include?
2) How do these product reviews describe the techniques and tools used to evaluate security and privacy?

III. Interviewing Product Reviewers

As we analyzed the content of published reviews, we found that many questions arose that could not be answered without information that was not published. Therefore, we are conducting semi-structured interviews with product reviewers, focusing on the following research questions:

1) To what extent do product reviewers currently evaluate security and privacy? What are their reasons?
2) What criteria do they consider?
3) What techniques and tools do they use?
4) What challenges do they face in evaluating security and privacy? What tools do they need to be more effective?
5) How do they communicate findings and judgments about security and privacy to consumers?

We are recruiting through a mix of methods: direct emails to individual product reviewers, word of mouth through industry contacts, and snowball sampling. We will record, transcribe, and code our conversations to facilitate qualitative analysis.

At the end of this project, we hope to inform the product review industry of potential areas for improvement in providing useful security and privacy advice to consumers. We also aim to recommend new tools and/or improvements to existing tools for evaluating security and privacy, in order to enhance usability and adoption among product reviewers. Finally, after understanding incentives and workflows particular to product reviewing, we hope to suggest research and development into how other professionals and institutions might complement product reviewers. We hope that this work will be just one step toward a new paradigm in which experts work in tandem to evaluate the security and privacy of Internet-connected devices, apps, and other software on behalf of consumers.

IV. Acknowledgements

This work results from the SPLICE research program, supported by a collaborative award from the National Science Foundation (NSF) SaTC Frontiers program under award numbers 1955805, 1955172, 1955228, and 1955231. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the NSF.

References

[1] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *Proceedings of the 26th USENIX Security Symposium*, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[2] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019. [Online]. Available: https://doi.org/10.1109/COMST.2019.2910750

[3] J. Reardon, Á. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman, "50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System," in *Proceedings of the 28th USENIX Security Symposium*, Aug. 2019, pp. 603–620. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

[4] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically Evaluating Security and Privacy for Consumer IoT Devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. New York, NY, USA: Association for Computing Machinery, Nov. 2017, pp. 1–6. [Online]. Available: https://doi.org/10.1145/3139937.3139938

[5] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. 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*. Glasgow: ACM, May 2019, pp. 1–12. [Online]. Available: https://dl.acm.org/doi/10.1145/3290605.3300764

[6] "The Digital Standard," 2020. [Online]. Available: https://thedigitalstandard.org/standard/

[7] K. Krippendorff, "Reliability in Content Analysis: Some Common Misconceptions and Recommendations," *Human Communication Research*, vol. 30, no. 3, pp. 411–433, 2004. [Online]. Available: https://doi.wiley.com/10.1093/hcr/30.3.411