Towards Automatic Identification and Blocking of Non-Critical IoT Traffic Destinations

Anna Maria Mandalari[1], Roman Kolcun[1], Hamed Haddadi[1], Daniel J. Dubois[2], and David Choffnes[2]

[1]Imperial College London
[2]Northeastern University

Extended Abstract

The consumer Internet of Things (IoT) space has experienced a significant rise in popularity in the recent years. From smart speakers, to baby monitors, and smart kettles and TVs, these devices are increasingly found in households around the world whose residents may be unaware of the risks associated with owning these devices. Previous work showed that these devices can threaten user privacy and security by exposing information over the Internet to a large number of service providers and third party analytics services. Our analysis shows that many of these Internet connections (and the information they expose) are neither critical, nor even essential to the operation of these devices. However, *automatically* separating out critical from non-critical network traffic for an IoT device is nontrivial, and at first glance would seem to require expert analysis based on manual experimentation in a controlled setting.

In this work, we ask whether it is possible to automatically classify network traffic destinations as either critical (essential for devices to function properly) or not, hence allowing the home gateway to act as a firewall to block undesired, non-critical destinations. We take the first steps towards designing and evaluating *IoTrimmer* [1], a framework for automated testing and analysis of various destinations contacted by devices, and selectively blocking the ones that do not impact device functionality.

Motivation. Privacy risks, at the network and application layers, have been extensively covered in previous research [2]–[4]. While a number of commercial *IoT Security* solutions are available for blocking malicious or otherwise undesirable connections, these often rely on user configuration for each device, and often provide an *all-or-nothing* connectivity option for traffic destinations without considering whether blocking traffic will break device functionality. There is a need for an approach that can block network traffic with little-to-no user configuration, and without breaking device functionality. Doing so can substantially reduce the privacy and security attack surfaces for IoT devices. A key requirement for this approach is to establish and maintain a list of network destinations that are essential for device functionality, and thus should not, in general, be blocked.

Design. To test *IoTrimmer*, we have built a testbed that currently comprises 122 different IoT devices in two labs, one in the US and one in the UK. The IoT devices can usually be controlled via a *companion device* such as a smartphone application. Our testbed allows us to perform automated experiments on the IoT devices using these companion devices and to capture several network traces for each device, retry destinations and perform self-validating automated experiments under different conditions. Finally, the testbed allows us to block traffic at device level by overriding DNS answers for specific hostnames using *bind*'s view and RPZ zones.

To detect the unnecessary destinations for an IoT device, we conduct interactions experiments. An IoT device can have different functionalities, for example switching on/off the light for a smart bulb is the main functionality, but the app can also provide an option for controlling the brightness. The interaction between the IoT device and the phone app may fail. As part of the interaction experiments, we created a tool for validating them using screenshots matching.

Evaluation. As a proof-of-concept study for *IoTrimmer*, we use three IoT devices: two security cameras and a smart bulb. By running more than 1,000 automated experiments, we find that some IoT devices contact non-critical destinations outside their region, and out of 9 destinations contacted by our three IoT devices, 4 are unnecessary.

Acknowledgments

We acknowledge constructive comments and feedback from the reviewers of IEEE S&P ConPro'20. This research was partially supported by the NSF CNS-1909020, the EPSRC Databox (EP/N028260/1), and the EPSRC Defence Against Dark Artefacts (EP/R03351X/1) grants.

References

[1] A. M. Mandalari, R. Kolcun, H. Haddadi, D. J. Dubois, and D. Choffnes, "Towards automatic identification and blocking of non-critical iot traffic destinations," *arXiv preprint arXiv:2003.07133*, 2020.

[2] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach," in *Proceedings of the Internet Measurement Conference*, 2019.

[3] H. Mohajeri Moghaddam, G. Acar, B. Burgess, A. Mathur, D. Y. Huang, N. Feamster, E. W. Felten, P. Mittal, and A. Narayanan, "Watching you watch: The tracking ecosystem of over-the-top tv streaming devices," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019.

[4] J. Varmarken, H. Le, A. Shuba, A. Markopoulou, and Z. Shafiq, "The tv is smart and full of trackers: Measuring smart tv advertising and tracking," *Proceedings on Privacy Enhancing Technologies*, vol. 2, pp. 129–154, 2020.