

W3C Web of Things Security Model

Michael McCool
Intel Corporation
michael.mccool@intel.com

Elena Reshetova
Intel Corporation
elena.reshetova@intel.com

Abstract—The W3C Web of Things (WoT) WG has been developing an interoperability standard for IoT devices that includes as its main deliverable a “Thing Description”: a standardized representation the metadata of an IoT device, including in particular its network interface, but also allowing for semantic annotation. In this paper, we discuss the implications of standardized metadata on security. Standardized metadata has both risks and opportunities. On the one hand, information about what devices can do makes it easier to scan for devices with vulnerabilities. However, this risk can in fact be an opportunity as scanning for devices with vulnerabilities is necessary to identify devices whose vulnerabilities need to be mitigated.

Pervasive metadata has one major additional benefit: it enables end-to-end security in multistandards networks. Specifically, if metadata is used to push payload adaptation to endpoints then the need to unpack and reformat data in gateways can be eliminated, and payloads can be encrypted end-to-end. This contrasts with systems that use local bridging between multiple IoT standards which requires opening (and usually deencrypting) data in potentially-vulnerable gateways.

The metadata also needs to be secured. Thing descriptions can be delivered from devices themselves, or from directory services. Directory services can also support discovery, including discovery based on semantic search. This raises the problem of how discovery can be constrained to return data that the searcher is authorized to access.

I. INTRODUCTION

II. CONCLUSION

ACKNOWLEDGMENT

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author's employer if the paper was prepared within the scope of employment.

NDSS '18, 18-21 February 2018, San Diego, CA, USA
Copyright 2018 Internet Society, ISBN 1-1891562-49-5
<http://dx.doi.org/10.14722/ndss.2018.23xxx>