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

Introduce us, please.

II. Related Work

Some relevant prior work: State-of-the-Art and Challenges for the Internet of Things Security [2]. The Industrial Internet of Things Security Framework [7]. IoT Security Foundation Best Practices Guidelines [1].

III. Web of Things Architecture

Web of Things architecture [4], Thing Description [3] and scripting API [5].

IV. Threat Model

A basic intro to to the WoT threat model [6].

V. Scenarios

Usage scenarios.

VI. Vulnerability Scanning

Vulnerability scanning using metadata.

VII. Endpoint Adaptation

End-to-end secure adaptation by pushing payload transformation to endpoints.

VIII. Secure Discovery

Secure semantic searches. How do we ensure only the data permitted for a user is used in a search? Some possibly relevant papers: [8], [9].

IX. Security Metadata

Metadata for distributed security and payment mechanisms.

X. Conclusion

Conclusions. What are the main points?

Acknowledgment

Thank you, thank you, all!

References

[1] "IoT security foundation best practice guidelines," IoT Security Foundation, Tech. Rep., May 2017. [Online]. Available: https://iotsecurityfoundation.org/best-practice-guidelines/

[2] O. Garcia-Morchon, S. Kumar, and M. Sethi, "State-of-the-art and challenges for the internet of things security," Working Draft, IETF Secretariat, Internet-Draft draft-irtf-t2trg-iot-seccons-08, Oct. 2017. [Online]. Available: http://www.ietf.org/internet-drafts/draft-irtf-t2trg-iot-seccons-08.txt

[3] S. Käbisch and T. Kamiya, "Web of things (WoT) thing description," W3C, W3C Working Draft, Sep. 2017. [Online]. Available: https://www.w3.org/TR/2017/WD-wot-thing-description-20170914/

[4] K. Kajimoto, U. Davuluru, and M. Kovatsch, "Web of things (WoT) architecture," W3C, W3C Working Draft, Sep. 2017. [Online]. Available: https://www.w3.org/TR/2017/WD-wot-architecture-20170914/

[5] Z. Kis, K. Nimura, and D. Peintner, "Web of things (WoT) scripting API," W3C, W3C Working Draft, Sep. 2017. [Online]. Available: https://www.w3.org/TR/2017/WD-wot-scripting-api-20170914/

[6] E. Reshetova and M. McCool, "Web of things (WoT) security and privacy considerations," W3C, W3C Note, Sep. 2017. [Online]. Available: https://www.w3.org/TR/2017/WD-wot-security-20171116/

[7] S. Schrecker, H. Soroush, J. Molina, M. Buchheit, J. LeBlanc, R. Martin, F. Hirsch, A. Ginter, H. Banavara, S. Eswarahally, K. Raman, A. King, Q. Zhang, P. MacKay, and B. Witten, "The industrial internet of things security framework," Industrial Internet Consortium, Tech. Rep. IIC:PUB:G4:V1.0:PB:20160926, Sep. 2016. [Online]. Available: http://www.iiconsortium.org/IISF.htm

NDSS '18, 18-21 February 2018, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2018.23xxx

[8] B. Thuraisingham, "Security standards for the semantic web," *Computer Standards and Interfaces*, vol. 27, no. 3, pp. 257 – 268, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548904000686

[9] Z. Xia, Y. Zhu, X. Sun, and L. Chen, "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking," *Journal of Cloud Computing*, vol. 3, no. 1, p. 8, Jul 2014. [Online]. Available: https://doi.org/10.1186/s13677-014-0008-2