Distributed Security Risks and Opportunities in the W3C Web of Things

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. Relative to other approaches to IoT, such metadata has at least four major implications. First, it allows for system-wide vulnerability analysis, which can be both a risk and an opportunity. Second, metadata can enable end-to-end security in multistandards networks, avoiding exposing data within bridges otherwise needed for connecting standards pairwise. Third, metadata supports service and device discovery, which raises the question of how to limit discovery to authorized agents. Fourth, metadata can enable distributed security mechanisms for access control and micropayments. To the extent that metadata access can be decentralized, decentralized mechanisms for security can be supported, although several practical issues currently make this difficult to fully support.**

I. Introduction

The economic impact of the IoT is strongly influenced by how well devices from different manufacturers can interoperate. Very often interoperability is taken for granted when estimating the business benefit of IoT. However, if devices do *not* interoperate, a recent study [6] concluded that 40% to 60% of the benefit of IoT will be unattainable, due to use cases that cannot be satisfied by a single manufacturer.

Unfortunately full interoperability is hard to acheive. There are currently many competing IoT standards under development. Most of these standards are prescriptive. In a prescriptive standard, devices are validated against specific requirements and typically the goals is that devices satisfying that standard will interoperate. In addition, it is possible to bridge multiple standards so that devices validated against one such standard can communicate with devices using another standard by translating communication protocols and payloads. Of course if one standard comes to dominate bridging will be unnecessary, but so far such unification seems to be elusive and may be impossible due to divergent requirements in different but overlapping IoT subdomains.

Unfortunately the prescriptive approach has some weaknesses. In particular, there are always going to be devices that follow older standards. There are decades-old devices in particular domains, such as building and factory automation, that are just now being connected to the IoT. These devices often represent major investments and cannot be economically replaced with newer, standards-conforming devices. This is the "brownfield" problem. In addition, new devices are being deployed today that have not been validated against any particular IoT standard, even if they use other standards such as JSON and HTTP.

As an alternative to the prescriptive approach, the W3C Web of Things (WoT) Working Group has been developing a *descriptive* approach to IoT interoperability. In this approach, metadata is provided that describes how to communicate with each particular device. The metadata itself is standardized but flexible enough to describe a wide variety of IoT network interfaces. With this approach, devices can but do not have to be prevalidated against a particular standard before being deployed. They can be described after the fact, and do not need any modification to be used as part of a Web of Things system. This solves the brownfield problem and allows older devices as well as devices satisfying different IoT standards to be integrated into a unified system.

This approach has both risks and opportunities from a security point of view.

Most obviously, IoT devices, even those conforming to a prescriptive IoT standard, may vary widely in their support for security. Therefore a Web of Things system needs to manage different levels of trust for different devices. Devices from different ecosystems or manufacturers may also take different approaches to security and may use different security mechanisms. This may cause integration challenges, even if the necessary information is provided in the metadata.

Beyond this basic concern, pervasive metadata raises several other issues from a security perspective. In this paper we discuss four major issues:

- **Vulnerability analysis:** Providing information about what devices can do makes it easier to automatically scan for devices with vulnerabilities. An attacker may also use this information to plan attacks that take advantage of vulnerabilities in multiple devices. However, for the

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

system manager, scanning can also be an opportunity to identify devices whose vulnerabilities need to be mitigated.
- **End-to-end security:** Metadata enables end-to-end security in networks of IoT devices using multiple standards. If metadata is used to push payload adaptation to endpoints then communication payloads can be encrypted end-to-end. This contrasts with systems that use local bridging to connect devices from multiple IoT standards. Local bridges require opening (and usually deencrypting) data in potentially-vulnerable gateways.
- **Secure discovery:** Information about how to use a service, and ideally even its existence, should not be disclosed to agents without the authorization to use it. The WoT approach allows powerful semantic searches to be used for discovery. How can this capability be made available while still securing the metadata?
- **Security mechanism enabling:** Metadata may be provided to enable specific security mechanisms, as well as features with security implications such as payment or scripting. What mechanisms are needed and what data needs to be provided? Also, depending on how the metadata is made available, it may or may not be possible to support decentralized approaches to security.

The next few sections first introduce the W3C Web of Things draft standard, focusing on the Thing Description metadata format. Then the security model for the WoT will be introduced, which includes a model of stakeholders, assets, attackers, and threats. Once this context has been established, we will discuss in detail the above four issues.

II. Web of Things

A. Architecture

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

B. Threat Model

A basic intro to to the WoT threat model [7].

C. Usage Scenarios

Usage scenarios.

III. 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 [8]. IoT Security Foundation Best Practices Guidelines [1].

IV. Risks and Opportunities

A. Local Links

Practical pitfalls. HTTPS not working locally. Local links vs global links in Thing Directories.

B. Vulnerability Scanning

Vulnerability scanning using metadata.

C. Endpoint Adaptation

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

D. 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: [9], [10].

E. Enabling Distributed Security

Metadata for distributed security and payment mechanisms. Tokens. Interledger addresses. Nested security.

V. Conclusion

We have given a summary of the W3C Web of Things draft standard, with a focus on the Thing Description. The Thing Description provides a descriptive approach to interoperability, which contrasts with the prescriptive approach of most other standards. While a prescriptive approach is useful, for example to enforce minimum security requirements, a descriptive approach can support brownfield devices and can also make it easier to integrate devices that conform to different prescriptive standards.

However, beyond the basic issue of integrating devices with different levels and mechanisms for security, which will arise with any multistandard IoT system, the use of descriptive metadata raises several new security risks and opportunities. We have discussed four such points: multidevice vulnerability analysis, end-to-end security enabling, secure discovery for semantic interoperability, and (potentially decentralized) security mechanism enabling.

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] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "The internet of things: Mapping the value beyond the hype," McKinsey Global Institute, Tech. Rep., Jun. 2015. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
[7] 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/

[8] 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

[9] 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

[10] 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