Network Working Group
Internet-Draft
Intended status: Informational
Expires: 27 January 2022

E. Nordmark
Zededa

26 July 2021

Different aspects of onboarding for IoT/Edge Devices
draft-nordmark-iotops-onboarding-00

Abstract

Previous onboarding discussions have focused on network onboarding. In this note we put that in the context of the larger onboarding picture to also discuss the onboarding to some management or orchestration system.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 27 January 2022.

Table of Contents

1. Introduction

The iotops group has discussed LwM2M [oma], FIDO [fidospec] and [I-D.lear-iotops-deep-thoughts-on-onboarding] where the last one intentionally focuses on network onboarding. This note broadens the discussion to all aspects of onboarding of IoT and edge devices to try to expose what is common and different at different layers.

Some of these topics has previously come up in T2TRG for example in [I-D.irtf-t2trg-secure-bootstrapping] but also with a strong networking focus.

2. What is onboarding?

One aspect of onboarding a device is providing network access to the device. That might involve both L2 and L3 aspects, such as Cellular and WiFi credentials at L2 and LAN as Internet access at L3. Furthermore, the L3 access might differentiate between LAN and Internet access and be subject to access control for instance controlled by MUD [RFC8520].

However, there are also higher levels of onboarding. For instance, Anima supports a notion of Secure Bootstrap over an Unconfigured Network [RFC8994] which not only includes the secure keys (BRSKI [RFC8995]) but also the configuration of the routers and switches (using GRASP [RFC8990]). Such configuration can have rather wide span and one can think of it as consisting of configuring the device plus configuring various applications (which might be routing protocols and management agents in the case of Anima use cases).

If we look at more compute-centric workloads are likely to have a larger set of applications which might be configured and managed separately from the device. We can already see examples of this in cloud datacenters where there is a IaaS layer provisioning and managing the servers, which is largely invisible to the users, and a set of applications (in the form for virtual machines or containers)

which are provisioned and managed using application-specific mechanisms and management systems. For instance, a firewall virtual appliance/VNF might be managed the same way as a physical firewall appliance.

3. IoT vs. Edge Computing?

The IOTOPS charter scopes its use of "IoT devices" to devices that

* are networked, either to the Internet or within limited administrative domains

* have a very limited end user interface or no end-user interface at all

* are deployed in sufficiently large numbers that they cannot easily be managed or maintained manually

The definitions of the various parts of Edge Computing by the Linux Foundation in [lfedge-wp] defines the constrained device edge and the smart device edge, which captures devices with different levels of flexibility, but they both fit into the above IOTOPS scope. Thus for the purposes of this discussion we can use Edge Computing devices and IoT devices interchangeably.

However, the devices at the constrained device edge are more likely to be single or fixed function in that they do not have the capacity or flexibility to perform other functions than envisioned prior to their deployment. Such fixed function devices still require a software/firmware update capability as discussed in [RFC8240], but they do not require handling new application deployment and associated new communication patterns.

The more flexible devices at the smart device edge are likely to be larger than the class 2 devices defined in [RFC7228], however if applications are sufficiently small, constrained devices might very well be edge computing devices. But in general it makes sense to think about devices of the Raspberry Pi class and larger at the smart device edge.

For such devices it is clear that the onboarding of the device (to the network and to some management system or controller) should be separable from the onboarding of some particular application (to its controller or management system). Hence the separation between device onboarding and application (instance) onboarding seems required from an architectural perspective.

4. Network onboarding

Network onboarding starts at L2 access and can take several different forms such as:

* Physical access to an Ethernet port

* Protocols like EAP-NOOB [I-D.ietf-emu-eap-noob], DPP [dpp], etc.

In the world of laptop computers and smartphones such access might include traditional EAP but also additional steps such as Endpoint Assessment [RFC5209][RFC7632] before granting full access to the network. Thus the onboarding to the network is not a new thing; what is new is applying it to IoT and Edge Computing devices with to user in front of the device as it is onboarded.

As indicated above, if MUD [RFC8520] is used the network onboarding would logically include the retrieval and application of the usage descriptions.

5. Security Considerations

This informational note discusses onboarding with the assumption that onboarding needs to address various security threats, but does not go into details.

It seems like the roots of trust used for onboarding at the different levels relates closely to the design center for the different onboarding approaches. Loosely we seem to have a few differently approaches (and this list is not exhaustive):

* Use Hardware manufacturer certificates. This makes it possible to verify with the manufacturer that device is valid, but it does not indicate which management system or controller which a device should trust.

* Track the transfers of ownership through supply chain as done in FIDO [fidospec]. This enables secure late binding to a management system/controller since the signature chain from manufacturer to end user establishes trust in controller.

* Imprinting/configuring for/by the owner of the device. This makes assumptions that either the future owner is known at the time of manufacturing or that there is some leap of faith involving a certificate (in e.g., text or bar code form) being registered in the controller by someone claiming to be the device owner.

The trust might also include initial measurement/attestation of firmware/software along the lines of RATS [I-D.ietf-rats-tpm-based-network-device-attest] to create a baseline before the device leaves the factory.

6. Example: Project EVE

Project EVE [eve] is an example of a secure but minimal approach to enable secure onboarding, without having a hard dependency on manufacturers and manufacturer certificates.

* When software is installed (factory or elsewhere):
  - Imprint device which controller to trust (a root certificate) and initial URL to contact
  - Generate a device certificate using the TPM
  - Extract the device certificate and pass to final user (paper, bar code, etc)
  - Perform initial measured boot to get baseline measurements along the lines of RATS TPM [I-D.ietf-rats-tpm-based-network-device-attest]
* Then in any order
  - User registers device certificate in controller
  - Device is installed and powered on and connects to its controller

At that point in time the EVE controller can specify which applications to deploy/boot/halt on device.

Potentially EVE can also leverage [sdo], which is an open source implementation of the FIDO specification [fidospec], for the future cases where there is sufficient support in the supply chain for the FIDO signature chains.

7. IANA Considerations

There are no IANA actions needed for this document.

8. Informative References

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", RFC 5209, DOI 10.17487/RFC5209, June 2008, <https://www.rfc-editor.org/info/rfc5209>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC7632] Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment: Enterprise Use Cases", RFC 7632, DOI 10.17487/RFC7632, September 2015, <https://www.rfc-editor.org/info/rfc7632>.

[RFC8240] Tschofenig, H. and S. Farrell, "Report from the Internet of Things Software Update (IoTSU) Workshop 2016", RFC 8240, DOI 10.17487/RFC8240, September 2017, <https://www.rfc-editor.org/info/rfc8240>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

[RFC8990] Bormann, C., Carpenter, B., Ed., and B. Liu, Ed., "GeneRic Autonomic Signaling Protocol (GRASP)", RFC 8990, DOI 10.17487/RFC8990, May 2021, <https://www.rfc-editor.org/info/rfc8990>.

[RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <https://www.rfc-editor.org/info/rfc8994>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

[I-D.lear-iotops-deep-thoughts-on-onboarding] Lear, E., "Deep Thoughts on Network Onboarding Challenges", Work in Progress, Internet-Draft, draft-lear-iotops-deep-thoughts-on-onboarding-00, 9 March 2021, <https://datatracker.ietf.org/doc/html/draft-lear-iotops-deep-thoughts-on-onboarding-00>.

[I-D.irtf-t2trg-secure-bootstrapping]
Sethi, M., Sarikaya, B., and D. Garcia-Carrillo, "Secure IoT Bootstrapping: A Survey", Work in Progress, Internet-Draft, draft-irtf-t2trg-secure-bootstrapping-00, 7 April 2021, <https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-secure-bootstrapping-00>.

[I-D.ietf-emu-eap-noob]
Aura, T., Sethi, M., and A. Peltonen, "Nimble out-of-band authentication for EAP (EAP-NOOB)", Work in Progress, Internet-Draft, draft-ietf-emu-eap-noob-05, 12 July 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-emu-eap-noob-05>.

[I-D.ietf-rats-tpm-based-network-device-attest]
Fedorkow, G., Voit, E., and J. Fitzgerald-McKay, "TPM-based Network Device Remote Integrity Verification", Work in Progress, Internet-Draft, draft-ietf-rats-tpm-based-network-device-attest-07, 10 June 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-tpm-based-network-device-attest-07>.

[dpp] Wi-Fi Alliance, "Wi-Fi Device Provisioning Protocol (DPP)", Wi-Fi Alliance , 2018, <https://www.wi-fi.org/download.php?file=/sites/default/files/private/Device_Provisioning_Protocol_Specification_v1.1_1.pdf>.

[fidospec] FIDO Alliance, "FIDO Device Onboard Specification", December 2020, <https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-RD-v1.0-20201202.html>.

[oma] Open Mobile Alliance, "Lightweight Machine to Machine Technical Specification: Core", Open Mobile Alliance , June 2019, <http://www.openmobilealliance.org/release/LightweightM2M/V1_1_1-20190617-A/OMA-TS-LightweightM2M_Core-V1_1_1-20190617-A.pdf>.

[lfedge-wp]
Linux Foundation, "Sharpening the Edge: Overview of the LF Edge Taxonomy and Framework", 2020, <https://www.lfedge.org/wp-content/uploads/2020/07/LFedge_Whitepaper.pdf>.

[eve] Linux Foundation, "EVE is Edge Virtualization Engine", July 2021, <https://github.com/lf-edge/eve>.

[sdo] Linux Foundation, "Secure Device OnBoard", July 2021, <https://www.lfedge.org/projects/securedeviceonboard>.

Author's Address

Erik Nordmark
Zededa
Santa Clara, CA,
United States of America

Email: nordmark@sonic.net