

SUIT
Internet-Draft
Intended status: Standards Track
Expires: November 26, 2021

B. Moran
H. Tschofenig
Arm Limited
May 25, 2021

Strong Assertions of IoT Network Access Requirements
draft-moran-suit-mud-02

Abstract

The Manufacturer Usage Description (MUD) specification describes the access and network functionality required a device to properly function. The MUD description has to reflect the software running on the device and its configuration. Because of this, the most appropriate entity for describing device network access requirements is the same as the entity developing the software and its configuration.

A network presented with a MUD file by a device allows detection of misbehavior by the device software and configuration of access control.

This document defines a way to link a SUIT manifest to a MUD file offering a stronger binding between the two.

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 November 26, 2021.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction	2
2. Terminology	3
3. Architecture	3
4. Extensions to SUIT	4
5. Security Considerations	5
6. IANA Considerations	5
7. Normative References	5
Authors' Addresses	6

1. Introduction

Under [RFC8520], devices report a URL to a MUD manager in the network. RFC 8520 envisions different approaches for conveying the information from the device to the network such as:

- DHCP,
- IEEE802.1AB Link Layer Discovery Protocol (LLDP), and
- IEEE 802.1X whereby the URL to the MUD file would be contained in the certificate used in an EAP method.

The MUD manager then uses the the URL to fetch the MUD file, which contains access and network functionality required a device to properly function.

The MUD manager must trust the service from which the URL is fetched and to return an authentic copy of the MUD file. This concern may be mitigated using the optional signature reference in the MUD file. The MUD manager must also trust the device to report a correct URL. In case of DHCP and LLDP the URL is unprotected. When the URL to the MUD file is included in a certificate then it is authenticated and integrity protected. A certificate created for use with network access authentication is typically not signed by the entity that wrote the software and configured the device, which leads to conflation of local network access rights with rights to assert all network access requirements.

There is a need to bind the entity that creates the software and configuration to the MUD file because only that entity can attest the network access requirements of the device. This specification defines an extension to the SUIT manifest to include a MUD file (per reference or by value). When combining a manufacturer usage description with a manifest used for software/firmware updates (potentially augmented with attestation) then a network operator can get more confidence in the description of the access and network functionality required a device to properly function.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Architecture

The intended workflow is as follows:

- At the time of onboarding, devices report their manifest in use to the MUD manager.
- If the SUIT_MUD_container has been severed, the suit-reference-uri can be used to retrieve the complete manifest.
- The manifest authenticity is verified by the MUD manager, which enforces that the MUD file presented is also authentic and as intended by the device software vendor.

- Each time a device is updated, rebooted, or otherwise substantially changed, it will execute an attestation.
 - o Among other claims in the Entity Attestation Token (EAT) [I-D.ietf-rats-eat], the device will report its software digest(s), configuration digest(s), primary manifest URI, and primary manifest digest to the MUD manager.
 - o The MUD manager can then validate these attestation reports in order to check that the device is operating with the expected version of software and configuration.
 - o Since the manifest digest is reported, the MUD manager can look up the corresponding manifest.
- If the MUD manager does not already have a full copy of the manifest, it can be acquired using the reference URI.
- Once a full copy of the manifest is provided, the MUD manager can verify the device attestation report and apply any appropriate policy as described by the MUD file.

4. Extensions to SUIT

To enable strong assertions about the network access requirements that a device should have for a particular software/configuration pair, we include the ability to add MUD files to the SUIT manifest. However, there are also circumstances in which a device should allow the MUD to be changed without a firmware update. To enable this, we add a MUD url to SUIT along with a subject-key identifier, according to [RFC7093], mechanism 4 (the keyIdentifier is composed of the hash of the DER encoding of the SubjectPublicKeyInfo value).

The following CDDL describes the extension to the SUIT_Manifest structure:

```
? suit-manifest-mud => SUIT_Digest
```

The SUIT_Envelope is also amended:

```
? suit-manifest-mud => bstr .cbor SUIT_MUD_container
```

```
SUIT_MUD_container = {  
  ? suit-mud-url => #6.32(tstr),  
  ? suit-mud-ski => SUIT_Digest,  
  ? suit-mud-file => bstr  
}
```

The MUD file is included verbatim within the bstr. No limits are placed on the MUD file: it may be any RFC8520-compliant file.

5. Security Considerations

This specification links MUD files to other IETF technologies, particularly to SUIT manifests, for improving security protection and ease of use. By including MUD files (per reference or by value) in SUIT manifests an extra layer of protection has been created and synchronization risks can be minimized. If the MUD file and the software/firmware loaded onto the device gets out-of-sync a device may be firewalled and, with firewalling by networks in place, the device may stop functioning.

6. IANA Considerations

suit-manifest-mud must be added as an extension point to the SUIT manifest registry.

7. Normative References

[I-D.ietf-rats-eat]

Mandyam, G., Lundblade, L., Ballesteros, M., and J. O'Donoghue, "The Entity Attestation Token (EAT)", draft-ietf-rats-eat-09 (work in progress), March 2021.

[I-D.ietf-suit-manifest]

Moran, B., Tschofenig, H., Birkholz, H., and K. Zandberg, "A Concise Binary Object Representation (CBOR)-based Serialization Format for the Software Updates for Internet of Things (SUIT) Manifest", draft-ietf-suit-manifest-12 (work in progress), February 2021.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

[RFC7093] Turner, S., Kent, S., and J. Manger, "Additional Methods for Generating Key Identifiers Values", RFC 7093, DOI 10.17487/RFC7093, December 2013, <<https://www.rfc-editor.org/info/rfc7093>>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

[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>>.

Authors' Addresses

Brendan Moran
Arm Limited

EMail: Brendan.Moran@arm.com

Hannes Tschofenig
Arm Limited

EMail: hannes.tschofenig@arm.com