Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 19 November 2021

E. Lear
Cisco Systems
S. Rose
NIST

18 May 2021

Discovering And Accessing Software Bills of Materials
draft-ietf-opsawg-sbom-access-01

Abstract

Software bills of materials (SBOMs) are formal descriptions of what pieces of software are included in a product. This memo specifies a different means for SBOMs to be retrieved.

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 19 November 2021.

Table of Contents

1. Introduction

Software bills of material (SBOMs) are descriptions of what software, including versioning and dependencies, a device contains. There are different SBOM formats such as Software Package Data Exchange [SPDX] or CycloneDX[CycloneDX12].

This memo specifies means by which SBOMs can be advertised and retrieved.

The mechanisms specified in this document are meant to satisfy several use cases:

* A network-layer management system retrieving an SBOM from an IoT device as part of its ongoing lifecycle. Such devices may or may not have interfaces available to query SBOM information.

* An application-layer management system retrieving an SBOM in order to evaluate the posture of an application server of some form. These application servers may themselves be containers or hypervisors. Discovery of the topology of a server is beyond the scope of this memo.

To satisfy these two key use cases, SBOMs may be found in one of three ways:

* on devices themselves

* on a web site (e.g., via URI)

* through some form of out-of-band contact with the supplier.

In the first case, devices will have interfaces that permit direct SBOM retrieval. Examples of these interfaces might be an HTTP, COAP or [OpenC2] endpoint for retrieval. There may also be private interfaces as well.

In the second case, when a device does not have an appropriate interface to retrieve an SBOM, but one is directly available from the manufacturer, a URI to that information must be discovered.

In the third case, a supplier may wish to make an SBOM available under certain circumstances, and may need to individually evaluate requests. The result of that evaluation might be the SBOM itself or a restricted URL or no access.

To enable application-layer discovery, this memo defines a well-known URI [RFC8615]. Management or orchestration tools can query this well-known URI to retrieve a system's SBOM. Further queries may be necessary based on the content and structure of a particular SBOM.

To enable network-layer discovery, particularly for IOT-based devices, an extension to Manufacturer Usage Descriptions (MUD) may be used[RFC8520].

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.

1.1. Cases Not Addressed

[This section to be removed prior to publication]

A separate use case may be addressed in future versions of this document:

* Related to the application layer, software as a service may involve multiple backend systems, depending on many factors. One example might be a large cloud-based service that offers

spreadsheets, email, and document authoring and management. Depending on what service is being used, a different set of back end services may in turn be invoking different software that should be listed.

The reason why this use case isn't addressed here is that it may be better addressed inline within HTML. Further discussion is required.

1.2. How This Information Is Used

SBOMs are used for numerous purposes, including vulnerability assessment, license management, and inventory management. This memo provides means for either automated or semi-automated collection of that information. For devices that can output a MUD URL or establish a well-known URI, the mechanism may be highly automated. For devices that have a MUD URL in either their documentation or within a QR code on a box, the mechanism is semi-automated (someone has to scan the QR code or enter the URL).

Note that SBOMs may change more frequently than access control requirements. A change to software does not necessarily mean a change to control channels that are used. Therefore, it is important to retrieve the MUD file as suggested by the manufacturer in the cache-validity period. In many cases, only the SBOM list will have been updated.

1.3. SBOM formats

There are multiple ways to express an SBOM. When these are retrieved either directly from the device or directly from a web server, tools will need to observe the content-type header to determine precisely which format is being transmitted. Because IoT devices in particular have limited capabilities, use of a specific Accept: header in HTTP or the Accept Option in CoAP is NOT RECOMMENDED. Instead, backend tooling MUST silently discard SBOM information sent with a media type that is not understood.

1.4. Discussion points

The following is discussion to be removed at time of RFC publication.

* Is the model structured correctly?

* Are there other retrieval mechanisms that need to be specified?

* Do we need to be more specific in how to authenticate and retrieve SBOMs?

* What are the implications if the MUD URL is an extension in a certificate (e.g. an IDevID cert)?

2. The .well-known/sbom endpoint set

If a host offers this service, it will offer the RESTful endpoint beginning with "{ORIGIN}/.well-known/sbom/base".

3. The mud-sbom extension model extension

We now formally define this extension. This is done in two parts. First, the extension name "sbom" is listed in the "extensions" array of the MUD file. N.B., this schema extension is intended to be used wherever it might be appropriate (e.g., not just MUD).

Second, the "mud" container is augmented with a list of SBOM sources.

This is done as follows:

```
module: ietf-mud-sbom

  augment /mud:mud:
    +--rw sbom
       +--rw (sbom-type)?
          +--:(cloud)
          |  +--rw sboms* [version-info]
          |     +--rw version-info    string
          |     +--rw sbom-url?       inet:uri
          +--:(local-well-known)
          |  +--rw local-well-known?   empty
          +--:(contact-info)
          |  +--rw contact-uri         inet:uri
          +--:(openc2)
             +--rw openc2-uri          inet:uri
```

4. The mud-sbom augmentation to the MUD YANG model

```
<CODE BEGINS>
file "ietf-mud-sbom@2021-04-29.yang"
module ietf-mud-sbom {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-mud-sbom";
  prefix mud-sbom;

  import ietf-inet-types {
    prefix inet;
  }
  import ietf-mud {
```

```
    prefix mud;
  }

  organization
    "IETF OPSAWG (Ops Area) Working Group";
  contact
    "WG
     Web: http://tools.ietf.org/wg/opsawg/
     WG List: opsawg@ietf.org
     Author: Eliot Lear lear@cisco.com
     Author: Scott Rose scott.rose@nist.gov";
  description
    "This YANG module augments the ietf-mud model to provide for
     reporting of SBOMs.

     Copyright (c) 2020 IETF Trust and the persons identified as
     authors of the code.  All rights reserved.

     Redistribution and use in source and binary forms, with or
     without modification, is permitted pursuant to, and subject to
     the license terms contained in, the Simplified BSD License set
     forth in Section 4.c of the IETF Trust's Legal Provisions
     Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     This version of this YANG module is part of RFC XXXX
     (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
     for full legal notices.

     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 (RFC 2119) (RFC 8174) when, and only when,
     they appear in all capitals, as shown here.  ";

  revision 2021-04-29 {
    description
      "Initial proposed standard.";
    reference
      "RFC XXXX: Extension for MUD SBOM";
  }

  grouping mud-sbom-extension {
    description
      "SBOM extension grouping";
    container sbom {
      description
        "container of methods to get an SBOM.";
```

```
          choice sbom-type {
            description
              "SBOM type";
            case cloud {
              list sboms {
                key "version-info";
                description
                  "A list of SBOMs tied to different s/w
                   or h/w versions.";
                leaf version-info {
                  type string;
                  description
                    "The version to which this SBOM refers.";
                }
                leaf sbom-url {
                  type inet:uri;
                  description
                    "A statically located URI.";
                }
              }
            }
            case local-well-known {
              leaf local-well-known {
                type empty;
                description
                  "SBOM information is to be retrieved via
                    https from the host on port 443, at
                    https://{hostname}/.well-known/sbom, where
                    hostname is replaced with the host to which
                    this MUD extension refers.";
              }
            }
            case contact-info {
              leaf contact-uri {
                type inet:uri;
                mandatory true;
                description
                  "This MUST be either a tel, http, https, or
                   mailto uri schema that customers can use to
                   contact someone for SBOM information.";
              }
            }
            case openc2 {
              leaf openc2-uri {
                type inet:uri;
                mandatory true;
                description
                  "A link to the OpenC2 https RESTful
```

```
                    \t mapping.  The OpenC2 protocol is then
                         used to retrieve the SBOM";
              }
            }
          }
        }
      }

      augment "/mud:mud" {
        description
          "Add extension for SBOMs.";
        uses mud-sbom-extension;
      }
    }
    <CODE ENDS>
```

5. Examples

In this example MUD file that uses a cloud service, the Frobinator presents a location of the SBOM in a URL. Note, the ACLs in a MUD file are NOT required, although they are a very good idea for IP-based devices. The first MUD file demonstrates how to get the SBOM without ACLs, and the second has ACLs.

5.1. Without ACLS

```
{
  "ietf-mud:mud": {
    "mud-version": 1,
    "mud-url": "https://iot-device.example.com/dnsname",
    "last-update": "2019-01-15T10:22:47+00:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "device that wants to talk to a cloud service",
    "mfg-name": "Example, Inc.",
    "documentation": "https://frob.example.com/doc/frob2000",
    "model-name": "Frobinator 2000",
    "extensions" : [
       "sbom"
      ],
    "sboms" : { "sbom" : [
      {
         "version-info" : "FrobOS Release 1.1",
         "sbom-url" : "https://frob.example.com/sboms/f20001.1",
      }
    ]
    }
  }
}
```

5.2. Located on the Device

```
{
  "ietf-mud:mud": {
    "mud-version": 1,
    "mud-url": "https://iot-device.example.com/dnsname",
    "last-update": "2019-01-15T10:22:47+00:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "device that wants to talk to a cloud service",
    "mfg-name": "Example, Inc.",
    "documentation": "https://frob.example.com/doc/frob2000",
    "model-name": "Frobinator 2000",
    "extensions" : [
       "sbom"
      ],
    "sboms" : "sbom" : {
        "sbom-local" : "coaps:///.well-known/sbom",
      }
  }
}
```

5.3. SBOM Obtained from Contact Information

```
{
  "ietf-mud:mud": {
    "mud-version": 1,
    "mud-url": "https://iot-device.example.com/dnsname",
    "last-update": "2019-01-15T10:22:47+00:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "device that wants to talk to a cloud service",
    "mfg-name": "Example, Inc.",
    "documentation": "https://frob.example.com/doc/frob2000",
    "model-name": "Frobinator 2000",
    "extensions" : [
       "sbom"
      ],
    "sboms" : { "sbom" : {
         "contact-uri" : "mailto:sbom-requst@example.com",
      }
    }
  }
}
```

5.4. With ACLS

```
{
  "ietf-mud:mud": {
    "mud-version": 1,
    "mud-url": "https://iot-device.example.com/dnsname",
    "last-update": "2019-01-15T10:22:47+00:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "device that wants to talk to a cloud service",
    "mfg-name": "Example, Inc.",
    "documentation": "https://frob.example.com/doc/frob2000",
    "model-name": "Frobinator 2000",
    "extensions" : [
       "sbom"
      ],
    "sboms" : "sbom" : [
      {
         "version-info" : "FrobOS Release 1.1",
         "sbom-url" : "https://frob.example.com/sboms/f20001.1",
      },
    ],
   },
    "from-device-policy": {
      "access-lists": {
        "access-list": [
          {
```

```
              "name": "mud-96898-v4fr"
            },
            {
              "name": "mud-96898-v6fr"
            }
          ]
        }
      },
      "to-device-policy": {
        "access-lists": {
          "access-list": [
            {
              "name": "mud-96898-v4to"
            },
            {
              "name": "mud-96898-v6to"
            }
          ]
        }
      }
    },
    "ietf-access-control-list:acls": {
      "acl": [
        {
          "name": "mud-96898-v4to",
          "type": "ipv4-acl-type",
          "aces": {
            "ace": [
              {
                "name": "cl0-todev",
                "matches": {
                  "ipv4": {
                    "ietf-acldns:src-dnsname": "cloud.example.com"
                  }
                },
                "actions": {
                  "forwarding": "accept"
                }
              }
            ]
          }
        },
        {
          "name": "mud-96898-v4fr",
          "type": "ipv4-acl-type",
          "aces": {
            "ace": [
              {
```

```
              "name": "cl0-frdev",
              "matches": {
                "ipv4": {
                  "ietf-acldns:dst-dnsname": "cloud.example.com"
                }
              },
              "actions": {
                "forwarding": "accept"
              }
            }
          ]
        }
      },
      {
        "name": "mud-96898-v6to",
        "type": "ipv6-acl-type",
        "aces": {
          "ace": [
            {
              "name": "cl0-todev",
              "matches": {
                "ipv6": {
                  "ietf-acldns:src-dnsname": "cloud.example.com"
                }
              },
              "actions": {
                "forwarding": "accept"
              }
            }
          ]
        }
      },
      {
        "name": "mud-96898-v6fr",
        "type": "ipv6-acl-type",
        "aces": {
          "ace": [
            {
              "name": "cl0-frdev",
              "matches": {
                "ipv6": {
                  "ietf-acldns:dst-dnsname": "cloud.example.com"
                }
              },
              "actions": {
                "forwarding": "accept"
              }
            }
```

```
            ]
          }
        }
      ]
    }
  }
```

At this point, the management system can attempt to retrieve the SBOM, and determine which format is in use through the content-type header on the response to a GET request.

6. Security Considerations

SBOMs provide an inventory of software. If firmware is available to an attacker, the attacker may well already be able to derive this very same software inventory. Manufacturers MAY restrict access to SBOM information using appropriate authorization semantics within HTTP. In particular, if a system attempts to retrieve an SBOM via HTTP and the client is not authorized, the server MUST produce an appropriate error, with instructions on how to register a particular client. One example may be to issue a certificate to the client for this purpose after a registration process has taken place. Another example would involve the use of OAUTH in combination with a federations of SBOM servers.

Another risk is a skew in the SBOM listing and the actual software inventory of a device/container. For example, a manufacturer may update the SBOM on its server, but an individual device has not be upgraded yet. This may result in an incorrect policy being applied to a device. A unique mapping of a device's firmware version and its SBOM can minimize this risk.

To further mitigate attacks against a device, manufacturers SHOULD recommend access controls through the normal MUD mechanism.

7. IANA Considerations

7.1. MUD Extension

The IANA is requested to add "controller-candidate" to the MUD extensions registry as follows:

Extension Name: sbom
Standard reference: This document

7.2. Well-Known Prefix

The following well known URI is requested in accordance with [RFC8615]:

URI suffix: "sbom"
Change controller: "IETF"
Specification document: This memo
Related information: See ISO/IEC 19970-2 and SPDX.org

8. References

8.1. Normative References

[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>.

[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>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

8.2. Informative References

[CycloneDX12] cylonedx.org, "CycloneDX XML Reference v1.2", May 2020.

[OpenC2] Lemire, D., Ed., "Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0", July 2019, <https://docs.oasis-open.org/openc2/open-impl-https/v1.0/open-impl-https-v1.0.html>.

[SPDX] The Linux Foundation, "SPDX Specification 2.1", 2016.

Appendix A. Changes from Earlier Versions

Draft -00:

* Initial revision

Authors' Addresses

Eliot Lear
Cisco Systems
Richtistrasse 7
CH-8304 Wallisellen
Switzerland

Phone: +41 44 878 9200
Email: lear@cisco.com

Scott Rose
NIST
100 Bureau Dr
Gaithersburg MD, 20899
United States of America

Phone: +1 301-975-8439
Email: scott.rose@nist.gov