Workgroup: OPS Area Working Group
Internet-Draft:
draft-richardson-opsawg-securehomegateway-
mud-05
Published: September 8, 2020
Intended Status: Informational
Expires: March 12, 2021
Authors: M. Richardson
Sandelman Software Works
J. Latour
CIRA Labs
H. Habibi Gharakheili
UNSW Sydney

On loading MUD URLs from QR codes

Abstract

This informational document details the mechanism used by the CIRA Secure Home Gateway (SHG) to load MUD definitions for devices which have no integrated MUD (RFC8520) support.

RFCEDITOR please remove: Pull requests and edit welcome at: https://github.com/CIRALabs/securehomegateway-mud/tree/ietf

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 March 12, 2021.

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.

Table of Contents

1. Introduction

The Manufacturer Usage Description (MUD) [RFC8520] defines a YANG data model to express what sort of access a device requires to operate correctly. The document additionally defines three ways for the device to communicate the URL of the resulting JSON [RFC8259] format file to a network enforcement point: DHCP, within an X.509 certificate extension, and via LLDP.

Each of the above mechanism conveys the MUD URL in-band, and requires modifications to the device firmware. Most small IoT devices do not have LLDP, and often have very restricted DHCP clients. Adding the LLDP or DHCP options requires at least some minimal configuration change, and possibly entire new subsystems. Meanwhile, use of the PKIX certification extension only makes sense as part of a larger IDevID based [ieee802-1AR] deployment such as [I-D.ietf-anima-bootstrapping-keyinfra].

In the above cases these mechanisms can only be implemented by persons with access to modify and update the firmware of the device.

The MUD system was designed to be implemented by Manufacturers after all!

In the meantime there is a chicken or egg problem ([chickenegg]): no manufacturers include MUD URLs in their products as there are no gateways that use them. No gateways include code that processes MUD URLs as no products produce them.

The mechanism described here allows any person with physical access to the device to affix a reference to a MUD URL that can later be scanned by an end user.

Such an action can be done by * the marketing department of the Manufacturer, * an outsourced assembler plant, * value added resellers (perhaps in response to a local RFP), * a company importing the product (possibly to comply with a local regulation), * a network administrator (perhaps before sending devices home with employees, or to remote sites), * a retailer as a value added service.

The mechanism described herein uses a QRcode, which is informally described in [qrcode], but specifically leverages the data format from Reverse Logistics Association's [SQRL] system. This is an application of the 12N Data Identifier system specified by the ANSI MH10.8.2 Committee in a format appropriate for QRcodes as well as other things like NFCs transmissions.

QR code generators are available as web services ([qrcodewebservice]), or as programs such as [qrencode]. They are formally defined in [isoiec18004].

Section {#genericfirmware} summarizes the recommendations [I-D.richardson-opsawg-mud-acceptable-urls] section 2 ("Updating MUD URLs vs Updating MUD files"). The question as to whether the MUD file should be specific to a specific version of the device firmware is considered in the context of affixed external labels.

A third issue is that an intermediary (ISP, or third-party security service) may want to extend or amend a MUD file received from a manufacturer. In order to maintain an audit trail of changes, a way to encode the previous MUD URL and signature file (and status) is provided. (FOR DISCUSSION)

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. Protocol

This QRcode protocol builds upon the work by [SQRL]. That protocol is very briefly described in the next section. Then the list of needed Data Records to be filled in is explained.

3.1. The SQRL protocol

[SQRL] documents an octet protocol that can be efficiently encoded into QRcodes using a sequence of ASCII bytes, plus five control codes (see section 3.1 of [SQRL]): * <RS> Record Separator (ASCII 30) * <EoT> End of Transmission (ASCII 4) * <FS> Field Separator (ASCII 28) * <GS> Group Separator (ASCII 29) * <US> Unit Separator (ASCII 31), * Concatenation Operator (ASCII 43: "+").

Section 7.2 of [SQRL] gives the details, which can be summarized as:

1. The QR code header starts with:

"[)>" <RS> "06" <GS> "12N"

1. Include one or more Data Records. This consists of a four letter Field Identifiers followed by ASCII characters terminated with a <Unit Separator>.

2. End with:

<RS><EoT>

There are, additionally optional flags that may be present in every Data Record as described in section 7.4. As there is little use for this in the context of MUD URLs, they can likely be ignored by parsers that are not parsing any of the rest of the information. A parser that sees a Field Separator in the stream SHOULD ignore the characters collected so far and then continue parsing to get the user data.

Environment records, as described in section 7.4, look and act exactly as fields, with a special Field Identifier. They serve no purpose when looking for MUD information, and MAY be ignored.

3.2. Manufacturer Usage Descriptions in SQRL

3.2.1. B000 Company Name

The B000 Data Record is mandatory in [SQRL]. It should be an ASCII representation of the company or brand name. It should match the ietf-mud/mud/mfg-name in the MUD file.

3.2.2. B001 Product Name

The B001 Data Record is optional. It is the Product Name in ASCII. It's presence is strongly RECOMMENDED.

3.2.3. B002 Model Number

The B002 Data Record is optional in [SQRL], but is MANDATORY in this profile. It is the Model Name in ASCII. It should match the ietf-mud/mud/model-name in the MUD file, if it is present.

3.2.4. MUD URL Data Record

A new Field Identifier has been request from the RLA, which is "UXXX" (probably "U087") This record should be filled with the MUD URL. Shorter is better. Section 8.1 of [SQRL] has some good advice on longevity concerns with URLs.

The URL provided MUST NOT have a query (?) portion present.

3.2.5. MUD device MAC address

In order for the MUD controller to associate the above policy with a specific device, then some unique identifier must be provided to the MUD controller. The most actionable identifier is the Ethernet MAC address. [SQRL] section 9.10 defines the Data Record: "M06C" as the MAC address. No format for the MAC address is provided in the document.

The recommended format in order to conserve space is 12 or 16 hex octets. (16 octets for the newer IEEE OUI-64 format used in 802.15.4, and some next generation Ethernet proposals)

The parser SHOULD be tolerant of extra characters: colons (":"), dashes ("-"), and white space.

4. Generic URL or Version Specific URL

MUD URLs which are communicated in-band by the device, and which are programmed into the device's firmware may provide a firmware specific version of the MUD URL. This has the advantage that the resulting ACLs implemented are specific to the needs of that version of the firmware.

A MUD URL which is affixed to the device with a sticker, or etched into the case can not be changed.

Given the considerations of [I-D.richardson-opsawg-mud-acceptable-urls] section 2.1 ("Updating the MUD file in place"), it is prudent

to use a MUD URL which points to a MUD file which will only have new features added over time, and never removed.

When the firmware eventually receives built-in MUD URL support, then a more specific URL may be used.

Note that in many cases it will be third parties who are generating these QRcodes, so the MUD file may be hosted by the third party.

5. Privacy Considerations

The presence of the MUD URL in the QR code reveals the manufacturer of the device, the type or model of the device, and possibly the firmware version of the device.

The MAC address of the device will also need to be present, and this is potentially Personally Identifiable Information (PII). Such QRcodes should not be placed on the outside of the packaging, and only on the device itself, ideally on a non-prominent part of the device. (e.g., the bottom).

The QR code sticker should not placed on any part of the device that might become visible to machine vision systems in the same area. This includes security systems, robotic vacuum cleaners, anyone taking a picture with a camera. Such systems may store the picture(s) in such a way that a future viewer of the image will be able to decode the QR code, possibly through assembly of multiple pictures. Of course, the QR code is not, however, a certain indicator that the device is present, only that the QR code sticker that came with the device is present.

6. Security Considerations

To Be Determined.

7. IANA Considerations

This document makes no IANA actions.

8. Acknowledgements

This work was supported by the Canadian Internet Registration Authority (cira.ca).

9. History

Previous versions of this work leveraged the QRcode format from the WiFi Alliance DPP specification. This document no longer uses that.

10. References

10.1. Normative References

[qrcode] Wikipedia, "QR Code", December 2019, <https://en.wikipedia.org/wiki/QR_code>.

[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>.

[SQRL] Reverse Logistics Association, "SQRL Codes: Standardized Quick Response for Logistics, Using the 12N Data Identifier", February 2017, <https://rla.org/resource/12n-documentation>.

10.2. Informative References

[chickenegg] Wikipedia, "Chicken or the egg", December 2019, <https://en.wikipedia.org/wiki/Chicken_or_the_egg>.

[I-D.ietf-anima-bootstrapping-keyinfra] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", Work in Progress, Internet-Draft, draft-ietf-anima-bootstrapping-keyinfra-43, August 7, 2020, <http://www.ietf.org/internet-drafts/draft-ietf-anima-bootstrapping-keyinfra-43.txt>.

[I-D.richardson-opsawg-mud-acceptable-urls] Richardson, M., Pan, W., and E. Lear, "Authorized update to MUD URLs", Work in Progress, Internet-Draft, draft-richardson-opsawg-mud-acceptable-urls-01, June 16, 2020, <http://www.ietf.org/internet-drafts/draft-richardson-opsawg-mud-acceptable-urls-01.txt>.

[ieee802-1AR] IEEE Standard, "IEEE 802.1AR Secure Device Identifier", 2009, <http://standards.ieee.org/findstds/standard/802.1AR-2009.html>.

[isoiec18004]
ISO/IEC, "Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification (ISO/IEC 18004)", February 2015.

[qrcodewebservice] Internet, "QR Code Generators", December 2019, <https://duckduckgo.com/?q=QR+code+web+generator>.

[qrencode] Fukuchi, K., "QR encode", December 2019, <https://fukuchi.org/works/qrencode/index.html.en>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

Authors' Addresses

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Jacques Latour
CIRA Labs

Email: Jacques.Latour@cira.ca

Hassan Habibi Gharakheili
UNSW Sydney

Email: h.habibi@unsw.edu.au