6lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 4, 2019

M. Richardson
Sandelman Software Works

January 31, 2019

Manufacturer Usuage Description for quarantined access to firmware
draft-richardson-shg-mud-quarantined-access-00

Abstract

The Manufacturer Usage Description is a tool to describe the limited access that a single function device such as an Internet of Things device might need.

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 August 4, 2019.

Table of Contents

1. Introduction

The document details an extension to the Manufacturer Usage Description (MUD) mechanism to be able to mark one or more ACLs as being enabled even though the device has quaranteed.

2. Requirements Language

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant STuPiD implementations.

3. MUD file extensions

3.1. Tree Diagram

```
module: cira-shg-mud
  augment /m:mud:
    +--rw quaranteed-device-policy
       +--rw access-lists
          +--rw access-list* [name]
             +--rw name    -> /acl:acls/acl/name
```

3.2. YANG FILE

```
<CODE BEGINS> file "cira-shg-mud@2017-12-11.yang"
module cira-shg-mud {
  yang-version 1.1;

  namespace
    "urn:ietf:params:xml:ns:yang:ietf-shg-mud";
  prefix "shg";

  import ietf-mud {
    prefix m;
    description "This module defines the format for a MUD description";
    reference "RFC YYYY: MUD YANG";
  }

  organization "CIRALabs Secure Home Gateway project.";

  contact
   "WG Web:   <http://securehomegateway.ca/>
    WG List:  <mailto:securehomegateway@cira.ca>
    Author:   Michael Richardson
              <mailto:mcr+ietf@sandelman.ca>";

  description
   "This module extends the RFCXXXX MUD format to include two
   facilities: definition of an Access Control List appropriate
   to enable device upgrade only, and provide for a history of
   modifications by third-parties to the MUD file";

  revision "2017-12-11" {
    description
     "Initial version";
    reference
     "RFC XXXX: MUD profile for Secure Home Gateway Project";
  }

  augment "/m:mud" {
    description
      "Adds leaf nodes appropriate MUD usage in the
       Secure Home Gateway";

    container quaranteed-device-policy {
      description
        "The policies that should be enforced on traffic
         coming from the device when it is under quaranteen.
         These policies are usually a subset of operational policies
         and are intended to permit firmware updates only.
```

```
        They are intended to keep the device safe (and the network safe
        from the device) when the device is suspected of being
        out-of-date, but still considered sufficiently intact to be
        able to do a firmware update";
      uses m:access-lists;
    }
  }

}
```

<CODE ENDS>

4. Protocol Definition

4.1. Protocol Example

5. Security Considerations

6. Privacy Considerations

7. IANA Considerations

There are no IANA actions created by this document.

8. Acknowledgements

9. References

9.1. Normative References

[I-D.ietf-opsawg-mud]
Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", draft-ietf-opsawg-mud-25 (work in progress), June 2018.

[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>.

9.2. Informative References

[I-D.ietf-6tisch-dtsecurity-secure-join]
Richardson, M., "6tisch Secure Join protocol", draft-ietf-6tisch-dtsecurity-secure-join-01 (work in progress), February 2017.

[RFC8180] Vilajosana, X., Ed., Pister, K., and T. Watteyne, "Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration", BCP 210, RFC 8180, DOI 10.17487/RFC8180, May 2017, <https://www.rfc-editor.org/info/rfc8180>.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca