opsawg Working Group (if adopted)
Internet-Draft
Intended status: Standards Track
Expires: May 6, 2021

M. Richardson
Sandelman Software Works
M. Ranganathan
NIST

November 02, 2020

Manufacturer Usage Description for quarantined access to firmware
draft-richardson-shg-mud-quarantined-access-02

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.

Table of Contents

1. Introduction 2
2. Requirements Language 2
3. MUD file extensions 2
3.1. Tree Diagram 2
3.2. YANG FILE 2
4. Security Considerations 4
5. Privacy Considerations 4
6. IANA Considerations 4
7. Acknowledgements 4
8. Normative References 4
Authors' Addresses 4

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 been 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 enabled-ace-names* [ace-name] +-rw ace-name ->
/acl:acls/acl/aces/ace/name
```

3.2. YANG FILE

```
<CODE BEGINS> file "ietf-mud-quarantine@2019-12-27.yang"
module ietf-mud-quarantine {
  yang-version 1.1;

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

  import ietf-mud {
    prefix m;
```

```
    description "This module defines an extension to MUD to mark entries as
being needed during quarantine";
    reference "RFC YYYY: MUD YANG";
  }

  organization "IETF OPSAWG Working group.";

  contact
    "WG Web: <https://datatracker.ietf.org/wg/opsawg/>
     WG List: opsawg@ietf.org
    Author:   Michael Richardson
              <mailto:mcr+ietf@sandelman.ca>

    Author:   M. Ranganathan
              <mailto:mranga@gmail.com>";

  description
   "This module extends the RFC8520 MUD format to 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 "2019-12-27" {
    description
     "Initial version";
    reference
     "RFC XXXX: MUD profile with quarantined access";
  }

  augment "/m:mud" {
    description
       "Adds leaf nodes for marking ACLs that should be enabled during
quarantine";

    container quaranteed-device-policy {
      description
        "The policies that should be enforced on traffic
         coming from the device when it is under quarantine.
         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";
      list enabled-ace-names {
        key ace-name;
        leaf ace-name {
          type leafref {
```

```
      path "/acl:acls/acl:acl/acl:aces/acl:ace/acl:name";
    }
```

```
        }
      }
    }
  }
}
```

<CODE ENDS>

4. Security Considerations

TBD

5. Privacy Considerations

TBD

6. IANA Considerations

The following YANG modules need to be registered in the "YANG Module Names" registry:

```
Name: ietf-mud
URN: urn:ietf:params:xml:ns:yang:ietf-mud
Prefix: ietf-mud
Registrant contact: The IESG
Reference: [THIS DOCUMENT]
```

7. Acknowledgements

8. 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>.

[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

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

M. Ranganathan
NIST

Email: mranga@gmail.com