Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 5, 2016

E. Lear
Cisco Systems

March 04, 2016

Manufacturer Usage Description YANG Model
draft-lear-ietf-netmod-mud-01

Abstract

This memo specifies a YANG model to be used to generate and parse manufacturer usage descriptions. These descriptions are retrieved by network management systems in order to instantiate policies associated with those devices. This memo also specifies a well known URI suffix to indicate that a file contains XML derived from this model.

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 http://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 September 5, 2016.

Copyright Notice

Table of Contents

1. Introduction

Manufacturer Usage Descriptions (MUDs) provide advice to end networks on how to treat specific classes of devices. The MUD architecture is explained in [I-D.lear-mud-framework]. The files that are retrieved are intended to be closely aligned to existing network architectures so that they are easy to deploy. We make use of YANG [RFC6020] and XML because many network vendors have focused their network management efforts through this interface.

The YANG model specified here is an extension of [I-D.ietf-netmod-acl-model]. The extensions in this model allow for a manufacturer to express classes of systems that a manufacturer would find necessary for the proper function of the device. These classes are then instantiated into actual IP addresses through local processing.

Because manufacturers do not know who will be using their devices, it is important for functionality referenced in usage descriptions to be

relatively ubiquitous, and therefore, mature. Therefore, only a limited subset of NETCONF-like content is permitted.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. The MUD Model and Semantic Meaning

A MUD file consists of XML based on a YANG model. For purposes of MUD, the elements that can be modified are access lists as augmented by this model. Publishers of MUD files MUST NOT include elements that are not stated in either this memo or by [I-D.ietf-netmod-acl-model].

This module is structured into four parts. The first container holds information that is relevant to retrieval and validity of the MUD file itself. The second container augments the matching container of the ACL model to add several elements that are relevant to the MUD URI, or other otherwise abstracted for use within a local environment. The third container augments actions to add quality of service treatment. Finally, an additional container provides for some meta-information relating to why a rule might be in place.

```
  module: ietf-mud
   +--rw support-information
      +--rw last-update?      yang:date-and-time
      +--rw cache-validity?   uint32
      +--rw masa-server?      inet:uri
      +--rw is-supported?     boolean
  augment /acl:access-lists/acl:acl/acl:access-list-entries
          /acl:ace/acl:matches:
   +--rw manufacturer?        inet:host
   +--rw same-manufacturer?   boolean
   +--rw model?               string
   +--rw local-networks?      empty
   +--rw controller?          inet:uri
```

3. Element Definitions

The following elements are defined.

3.1. last-update

This is a date-and-time value of the last time the XML file was updated. This is akin to a version number.

3.2. cache-validity

This uint32 is the period of time in hours that a network management station MUST wait since its last retrieval before checking for an update. It is RECOMMENDED that this value be no less than 24 and no more than 144 for any device that is supported.

3.3. masa-server

This optional element refers to the URI that should be used to resolve the location any MASA service, as specified in [I-D.ietf-anima-bootstrapping-keyinfra].

3.4. is-supported

This boolean is an indication from the manufacturer to the network administrator as to whether or not the device is supported. In this context a device is said to be supported if the manufacturer might issue an update to the device or if the manufacturer might update the MUD file.

3.5. manufacturer

This element consists of a hostname that would be matched against the authority section of another device's MUD URI.

3.6. same-manufacturer

This is a boolean equivalent for when the manufacturer element is used to indicate the authority that is found in another device's MUD URI matches that of the authority found in this device's MUD URI.

3.7. model

This string matches the one and only segment following the authority section of the MUD URI. It refers to a model that is unique within the context of the authority. It may also include product version information. Thus how this field is constructed is entirely a local matter for the manufacturer.

3.8. local-networks

This null-valued element expands to include local networks. Its default expansion is that packets must not traverse toward a default route that is received from the router.

3.9. controller

This URI specifies a value that a controller will register with the network management station. The element then is expanded to the set of hosts that are so registered.

In addition, some meta information is defined in order to determine when a usage description should be refreshed. Finally, the class of a device may be specified, such that a generic policy for a given class may be applied.

An example of an intended MUD policy for a lightbulb might be as follows:

Allow access to controller "https://mfg.example.com/example-printers"
Allow access to local DNS/DHCP
Deny all other access

4. What does a MUD URI look like?

To begin with, MUD takes full advantage of both the https: scheme and the use of .well-known. HTTPS is important in this case because men in the middle could otherwise harm the operation of a class of devices. .well-known is used because we wish to add additional structure to the URI. And so the URI appears as follows:

```
   mud-uri   = "https://" authority  "/.well-known/mud/" mud-rev
               "/" model "/" dev-rev *( "?" extras )
           ; authority is from RFC3986
   mud-rev   = "v1"
   model     = segment  ; from RFC3986
   dev-rev   = segment  ; from RFC3986
   extras    = query    ; from RFC3986
```

mud-rev signifies the version of the manufacturer usage description file. This memo specifies "v1" of that file. It should be pointout that later versions may not use XML at all.

"model" represents a device model as the manufacturer wishes to represent it. It could be a brand name or something more specific. "dev-rev" provides a means to indicate what version the product is. Specifically if it has been updated in the field, this is the place where evidence of that update would appear. Once again, the field is opaque. From a controller standpoint, therefore, only comparison and matching operations are safe. Processing of this URI occurs as specified in [RFC2818] and [RFC3986].

5. The MUD YANG Model

```
<CODE BEGINS>file "ietf-mud.yang";

module ietf-mud {
  yang-version 1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-mud";
  prefix "ietf-mud";


  import ietf-access-control-list {
    prefix "acl";
  }

  import ietf-yang-types
  {
    prefix "yang";
  }

  import ietf-inet-types
  {
    prefix "inet";
  }

  organization
    "Cisco Systems, Inc.";

  contact
    "Eliot Lear
     lear@cisco.com
    ";

  description
    "This YANG module defines a component that augments the
     IETF description of an access list.  This specific module
     focuses on additional filters that include local, model,
     and same-manufacturer.
    Copyright (c) 2015 IETF Trust and the persons identified as
    the document authors.  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
    (http://trustee.ietf.org/license-info).
    This version of this YANG module is part of RFC XXXX; see
    the RFC itself for full legal notices.";
```

```
     revision "2015-12-15"  {
       description "A policy container for manufacturer-driven policy";
       reference "RFC XXXX";
     }


     container support-information
     {

       description "Information about when support end(ed), and
                    when to refresh";

       leaf last-update
       {
         type yang:date-and-time;
         description "This is intended to be the time and date that
                      the MUD file was generated.";
       }

       leaf cache-validity
       {
         type uint32;
         description "The information retrieved from the MUD server is
                    valid for these many hours, after which it should
                    be refreshed.";
       }

       leaf masa-server {
         type inet:uri;
         description "The URI of the MASA server that network
         elements should forward requests to for this device.";
       }

       leaf is-supported
       {
         type boolean;
         description "The element is currently supported
                      by the manufacturer.";
       }
     }


     augment "/acl:access-lists/acl:acl/" +
        "acl:access-list-entries/acl:ace/" +
        "acl:matches" {
       description "adding manufacturer-driven policy";

       leaf manufacturer
```

```
      {
        type inet:host;
        description "authority component of the manufacturer URI";
      }

      leaf same-manufacturer
      {
        type boolean;
        description "expand to ACEs for each device
                 with the same origin";
      }

      leaf model
        {
      type string;
      description "specific model for a given manufacturer";
        }

      leaf local-networks {
        type empty;
        description "this string is used to indicate networks
                     considered local in a given environment.";
      }
      leaf controller {
        type inet:uri;
        description "expands to one or more controllers for a
                     given service that is codified by inet:uri.";
      }
    }
  }

  <CODE ENDS>
```

6. Example

The example below permits access to devices that are registered with the MUD system of type "http://mfg.example.com/printers". It denies all other access.

```
<?xml version='1.0' encoding='UTF-8'?>
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <access-lists
   xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list"
   xmlns:ietf-acl-dnsname="urn:ietf:params:xml:ns:yang:ietf-mud">
       <acl>
        <access-list-entries>
          <ace>
            <matches>
          <controller>
             http://mfg.example.com/printers
          </controller>
            </matches>
            <actions>
              <permit />
            </actions>
            <rule-name>rule1<rule-name/>
          </ace>
        </access-list-entries>
        <acl-name>sample-mud-acl<acl-name/>
        <acl-type>ipv4-acl<acl-type/>
      </acl>
    </access-lists>
  </data>
```

7. Security Considerations

Based on the means a URI is procurred, a device may be able to lie about what it is, thus gaining additional network access. This will occur when it makes use of primitives such as "manufacturer" for the purpose of accessing devices of a particular type. Depending on the sophistication of the attack it will be easier or harder to detect. Network management systems SHOULD NOT deploy a usage description for a a device with the same MAC address that has indicated a change of authority without some additional validation (such as review of the class). New devices that present some form of unauthenticated MUD URI SHOULD be validated by some external means when they would be otherwise be given increased network access.

It may be possible for a rogue manufacturer to inappropriately exercise the MUD file parser, in order to exploit a vulnerability. There are two recommended approaches to address this threat. The first is to have a system do a primary scan of the file to ensure that it is both parseable and believable at some level. MUD files will likely be relatively small, to start with. The number of ACEs used by any given device should be relatively small as well. Second, it may be useful to limit retrieval of MUD URIs to only those sites that are known to have decent web reputations.

8. IANA Considerations

This memo will make a request of IANA for the URI suffix of ".mud". Specification to follow.

9. Acknowledgments

The author would like to thank Einar Nilsen-Nygaard for his valuable advice. The numerous remaining errors in this work are entirely the responsibility of the author.

10. References

10.1. Normative References

[I-D.ietf-anima-bootstrapping-keyinfra]
Pritikin, M., Richardson, M., Behringer, M., and S. Bjarnason, "Bootstrapping Key Infrastructures", draft-ietf-anima-bootstrapping-keyinfra-01 (work in progress), October 2015.

[I-D.ietf-netmod-acl-model]
Bogdanovic, D., Koushik, K., Huang, L., and D. Blair, "Network Access Control List (ACL) YANG Data Model", draft-ietf-netmod-acl-model-06 (work in progress), December 2015.

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

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <http://www.rfc-editor.org/info/rfc2818>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <http://www.rfc-editor.org/info/rfc6020>.

10.2. Informative References

[I-D.lear-mud-framework]
Lear, E., "Manufacturer Usage Description Framework", draft-lear-mud-framework-00 (work in progress), January 2016.

Author's Address

Eliot Lear
Cisco Systems
Richtistrasse 7
Wallisellen CH-8304
Switzerland

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