Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 28, 2017

B. Weis
Cisco Systems

October 25, 2016

RADIUS Extensions for Manufacturer Usage Description
draft-weis-radext-mud-00

Abstract

A Manufacturer Usage Description (MUD) is a file describing the expected use of a class of devices, usually an Internet of Things class of devices. It is prepared by a manufacturer and placed on a generally available web server, and is addressable via a Uniform Resource Identifier (URI). The URI is often included in a discovery protocol (e.g., DNS, LLDP). A Network Access Server (NAS) in the path of the discovery protocol can collect and forward the URI to a RADIUS server, which processes the URI. This draft defines the RADIUS extension needed for the NAS to forward the URI to the RADIUS server.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Enterprise networks often use Port-Based Network Access Control [IEEE802.1X], where the Authentication Server is a RADIUS server [RFC2865]. In some cases a device will authenticate itself to the network using IEEE 802.1X with a digital certificate (e.g., an IEEE 802.1AR Secure Device ID [IEEE802.1AR]) that has been placed into the device by the manufacturer. Manufacturer Usage Description (MUD) [I-D.ietf-opsawg-mud] has defined an optional extension for digital certificates, which consists of a Uniform Resource Identifier (URI) that identifies the MUD file. A MUD file contains identification and network access information for a particular class of device. This information can be used to generate authorization policy such as an Access Control List (ACL) describing required network access for the device.

However, there are cases where a MUD URI is not included in a device's digital certificate, or it does not support the use of digital certificates, or may not even support an IEEE 802.1X Supplicant. This will often be the case with IoT devices, which is a primary use case for the use of MUD. In each of these situations, a device could benefit from distributing a MUD URI in a discovery message (e.g., a DHCP or LLDP message as defined in [I-D.ietf-opsawg-mud]), in hopes that a network element device will receive and consume it.

As shown in Figure 1, a Network Access Server (NAS) can observe the discovery message with the MUD URI and forward it to a RADIUS server. This can be done as part of a MAC Authentication Bypass (MAB) message. MAB is a common alternative approach of port-based network access control used for devices that cannot support a IEEE 802.1X Supplicant. The RADIUS server and an associated MUD Controller (defined in [I-D.ietf-opsawg-mud]) will work together to resolve the URI and translate the resulting MUD file into authorization policy. The RADIUS server distributes to the NAS authorization RADIUS attributes (e.g., an ACL describing required network access) to apply to messages received from the device.

```
                                                RADIUS Server &
            Device            NAS               MUD Controller
              +                +                       |
              | (DHCP or LLDP) |                       |
              |     MUD URI    |                       |
              |  +-----------> |      (RADIUS)         |
              |                |  MUD URI ATTRIBUTE    |
              |                | +------------------->  |
              |                |                       |
              |                |   FILTER ATTRIBUTES   |
              |                | <--------------------+|
              +                +                       +
```

Figure 1: RADIUS Message Flow

The only missing piece in this workflow is the ability for the NAS to relay the MUD URI to the RADIUS server. This draft defines a new RADIUS attribute for this purpose. The expectation is that the MUD URI will be passed in Access Request or Accounting messages.

1.1. Requirements notation

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].

1.2. Terminology

The following key terms are used throughout this document:

MUD Controller An entity that requests a MUD file from the MUD server, and processes the MUD file upon receipt.

MUD file A file containing a MUD Yang file definition, as defined in [I-D.ietf-opsawg-mud]

MUD URI A URI pointing to a MUD file, typically located on a web server.

2. Acronyms and Abbreviations

The following acronyms and abbreviations are used throughout this document

DHCP	Dynamic Host Configuration Protocol
IoT	Internet of Things
LLDP	Link Layer Discovery Protocol
MAB	MAC Authentication Bypass
MUD	Manufacturer Usage Description
NAS	Network Access Server

3. Extended Attribute for the MUD URI

This attribute is of type "TLV" as defined in the RADIUS Protocol Extensions [RFC6929]. It is named the MUD-URI Attribute, and is defined in Figure 2.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |     Length    | Extended-Type |    Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: MUD TLV format

Type

TBD1

Length

This field indicates the total length in bytes of all fields of this attribute, including the Type, Length, Extended-Type, and the entire length of the Value.

Extended-Type

TBD2

Value

A MUD URI as defined in [I-D.ietf-opsawg-mud], and MUST conform to the syntax defined a URI [RFC3986].

4. MUD URI processing

When a NAS receives a MUD URI, it forwards it to a RADIUS server using the Extended Attribute described in Section 3.

When a RADIUS server receives a MUD URI, it works in conjunction with a MUD Controller to retrieve the MUD file and processes it as described in [I-D.ietf-opsawg-mud]. They determine filter policies based on the MUD file, and the RADIUS server passes these filter policies to the NAS using commonly used RADIUS filter attributes.

Finally, the NAS receives the RADIUS filter attributes and applies them to the network traffic associated with the new device.

5. Security Considerations

This document defines a RADIUS attribute, which does not affect the security considerations of the RADIUS protocol [RFC2865].

Security considerations regarding the integrity of the MUD URI are outside the scope of this document, but it may be helpful to consider how a network using MAB might use a MUD URI. When retrieved from an authenticated device a NAS does not absolutely know if this MUD file is correct for the device that proffers the MUD URI, but it can use the MUD file as a hint as to the type of device. A NAS may be able to correlate the claimed device type with other policy for this device using other mechanisms. It should also be noted that the intent of a MUD policy description is to severely limit the network access of the device (e.g., using filters), rather than grant wide access to a device. Therefore, the action of proffering a MUD URI indicates a willingness to have its network access restricted rather than opened.

6. IANA Considerations

TBD1: One of the RADIUS Types that indicates an Extended Type

TBD2: A RADIUS Extended Type value.

7. Acknowledgements

The author thanks Nancy Cam-Winget for her thoughtful review, which resulted in substantial improvements to the memo.

8. References

8.1. Normative References

[I-D.ietf-opsawg-mud]
Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", draft-ietf-opsawg-mud-01 (work in progress), September 2016.

[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>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <http://www.rfc-editor.org/info/rfc2865>.

[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>.

8.2. Informative Reference

[IEEE802.1AR]
IEEE Computer Society, "802.1AR-2009 - IEEE Standard for Local and metropolitan area networks--Secure Device Identity", February 2010, <https://standards.ieee.org/findstds/standard/802.1AR-2009.html>.

[IEEE802.1X]
IEEE Computer Society, "802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control", February 2010, <https://standards.ieee.org/findstds/standard/802.1X-2010.html>.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", RFC 6929, DOI 10.17487/RFC6929, April 2013, <http://www.rfc-editor.org/info/rfc6929>.

Author's Address

Brian Weis
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1 408 526 4796
Email: bew@cisco.com