Abstract

This document describes how Network Endpoint Assessment (NEA) data can be carried inside of an EAP method using EAP-TLV.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on July 9, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with 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 BSD License.

Table of Contents

1. Introduction ................................................. 3
2. Specification Requirements ................................. 3
3. EAP NEA TLV Format ........................................... 3
4. Capabilities and Limitations of EAP-TLV as a PT for PB-TNC .. 4
5. Security Considerations ....................................... 4
6. IANA Considerations .......................................... 5
7. Acknowledgements ............................................. 5
8. Normative References ......................................... 5
Authors’ Addresses .............................................. 5
1. Introduction

NEA has standardized a transport agnostic Posture Broker protocol defined in [I-D.ietf-nea-pb-tnc] to effect a network endpoint assessment between a Posture Broker Client and a Posture Broker Server. The Extensible Authentication Protocol (EAP) [RFC3748] defines an authentication transport mechanism that can be extended to transport the Posture Broker Protocol. [draft-cam-winget-eap-tlv-00] defines an EAP-TLV container to carry arbitrary data within an EAP method.

This document describes an EAP-TLV that can be used to carry Posture Broker messages within an EAP method. This document also describes the capabilities and limitations of EAP as a transport mechanism for carrying NEA protocols.

2. Specification Requirements

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].

3. EAP NEA TLV Format

The NEA EAP TLV Format is defined and described below. The fields are transmitted from left to right.

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|M|R|            TLV Type       |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                        PB-TNC Header                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        PB-PA Message....                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

M
0  Optional TLV

1  Mandatory TLV

R

Reserved, set to zero (0)

TLV Type

The EAP NEA TLV type:

TBD

Length

The length of the Value field in octets.

PB-TNC Header

The PB-TNC encapsulation header as described in [I-D.ietf-nea-pb-tnc].

PB-PA Message

The message between the Posture Broker Client and Posture Broker Server as described in [I-D.ietf-nea-pb-tnc].

4. Capabilities and Limitations of EAP-TLV as a PT for PB-TNC

TBD

5. Security Considerations

The EAP NEA TLV container carries network endpoint assessment information between the Posture Broker Client and the Posture Broker Server. As some of this data can be sensitive, it is highly recommended that the EAP NEA TLV container MUST be carried inside a protected EAP tunneled method.
6. IANA Considerations

The IANA is hereby requested to create a new registry for the EAP NEA TLV defined in Section 3. The purpose of this registry is uniquely identify when NEA Posture Broker Protocol packets are being transported in an EAP method.

7. Acknowledgements

The authors would like to recognize Joe Salowey, Susan Thomson, Syam Appala and Subbu Srinivasan for providing input into this draft.

8. Normative References

[I-D.ietf-nea-pb-tnc]


Authors’ Addresses

Nancy Cam-Winget
Cisco Systems
80 West Tasman Drive
San Jose, CA  95134
US

Email: ncamwing@cisco.com
Hao Zhou
Cisco Systems
4125 Highlander Parkway
Richfield, OH  44286
US

Email: hzhou@cisco.com