

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 7, 2011

N. Cam-Winget
H. Zhou
Cisco Systems
January 3, 2011

EAP TLV for NEA
draft-cam-winget-eap-nea-tlv-02

Abstract

This document describes how Network Endpoint Assessment (NEA) data can be carried inside of a general Type-Length-Value container using EAP-TLV.

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 July 7, 2011.

Copyright Notice

Copyright (c) 2011 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 Simplified BSD License.

This document may contain material from IETF Documents or IETF

Internet-Draft

EAP NEA TLV

January 2011

Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

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 . .	5
5.	Security Considerations	5
6.	IANA Considerations	5
7.	Acknowledgements	5
8.	Normative References	5
	Authors' Addresses	6

Internet-Draft

EAP NEA TLV

January 2011

1. Introduction

NEA has standardized a transport agnostic Posture Broker protocol defined in [RFC5793] 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-01] defines an EAP-TLV container to carry arbitrary data within an EAP method.

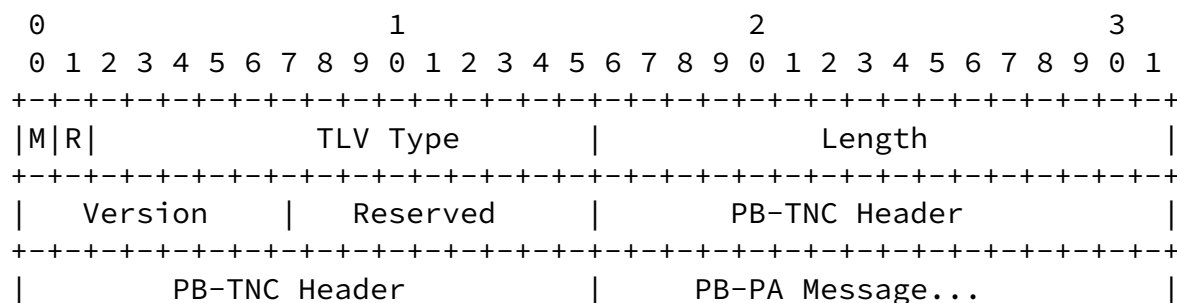
This document describes an EAP-TLV that can be used to carry Posture Broker messages within an EAP method. This document also describes the capabilities and limitations of EAP as a transport mechanism for carrying NEA protocols.

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.



```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|
|                                     PB-PA-Message...
|
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

M

Cam-Winget & Zhou

Expires July 7, 2011

[Page 3]

Internet-Draft

EAP NEA TLV

January 2011

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.

Version

The one octet version of the EAP NEA TLV:

1

Reserved

Reserved octet, must be set to 0x00

PB-TNC Header

The PB-TNC encapsulation header as described in [[RFC5793](#)].

PB-PA Message

The message between the Posture Broker Client and Posture Broker Server as described in [[RFC5793](#)].

[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.

To address the potential man-in-the-middle attack in a tunneled EAP method, the 'tls-unique' Channel Binding as defined in [[RFC5929](#)] MUST be used.

[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

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [RFC4493] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", [RFC 4493](#), June 2006.

- [RFC5793] Sahita, R., Hanna, S., Hurst, R., and K. Narayan, "PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC)", [RFC 5793](#), March 2010.
- [RFC5929] Altman, J., Williams, N., and L. Zhu, "Channel Bindings for TLS", [RFC 5929](#), July 2010.

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