Abstract

This document specifies a new message TLV for AODVv2 and, potentially, other reactive protocols. The new message TLV allows the endpoints of a newly discovered route to be assured that they were the originator of the RREQ and responder producing the RREP respectively.

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 4, 2016.

Copyright Notice

Copyright (c) 2016 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.
1. Introduction

Hop-by-hop security for AODV relies on transitive trust between the nodes during route discovery. In case that some of the nodes may become compromised, it would be useful for the source and destination nodes for the discovered routes to be assured that they both participated in the route discovery process, and thus that a route was indeed established between them. This does not guarantee a functioning route because malicious intermediate nodes might still misdirect or drop traffic.

2. Terminology

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

This document also uses some terminology from [RFC5444] and AODVv2 [I-D.ietf-manet-aodvv2].

3. Algorithm for computing the Message TLV authenticator data

The authentication algorithm uses HMAC-SHA-256-128 [RFC4868] to compute authentication data. The input data for the computation is the concatenation of the following information contained in an AODVv2 [I-D.ietf-manet-aodvv2] message:

- OrigAddr
- TargAddr
- PrefixLengthList if present in the message
- OrigSeqNum if present in the message
- TargSeqNum if present in the message
- MetricType
The output of the computation is a 128-bit authenticator value which is used for the value field of the E2E Authenticator Message TLV.

4. Format for the E2E Authenticator Message TLV

The format for the E2E Authenticator Message TLV is shown in Figure 1.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Flags      |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Authenticator (128 bits)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Format for E2E Authenticator Message TLV

Type
The E2E Authenticator Message TLV type

Flags
MUST be transmitted as zero and ignored on reception.

Authenticator
128 bits authentication data computed as described in Section 3.

5. Security Considerations

This document introduces a security mechanism to enable the two endpoints of a route discovery operation to verify that they are using the same immutable data elements as were supplied by the node generating the Route Discovery message (i.e., RREQ or RREP). This should provide additional security to protect against creation of routes to a destination when no such route exists.

6. IANA Considerations

This document specifies the designation of a new Message TLV Type to be allocated from the "Message TLV Types" namespace defined in [RFC5444].

6.1. Acknowledgement

This document has benefitted from comments by Vicky Mercieca and from other discussion with the AODVv2 author team.
7. Normative References


Author’s Address

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA  95050
USA

Phone: +1-408-330-4586
Email: charliep@computer.org