IPv6 Authentication Header with Segment Routing Header Processing
draft-herbert-ipv6-srh-ah-00

Abstract

This specification describes processing of the IPv6 Authentication Header when the IPv6 Segment Routing Header is present in the same packet. Specifically, the handling of mutable fields in the Segment Routing Header for the purposes of computing or verifying the packet’s authenticating value is specified.

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/1id-abstracts.html

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

Copyright and License Notice

Copyright (c) 2019 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
Table of Contents

1 Introduction ........................................ 3
1.1 Handling mutable fields in AH ................. 3
1.2 Mutable fields in Segment Routing Header .... 3
2 Handling mutable SRH fields for ICV calculation ... 4
3 Security Considerations ............................ 5
4 IANA Considerations ................................. 5
5 References ........................................... 5
  5.1 Normative References ............................. 5
  5.2 Informative References ............................ 5
Author’s Address ...................................... 5
1 Introduction

This specification describes processing of the IPv6 Authentication Header (AH) [RFC4302] when the IPv6 Segment Routing Header (SRH) [SRH] is present in the same packet. AH is used to authenticate the preceding IPv6 header and extension headers in a packet. Authentication is performed by computing an Integrity Check Value (ICV) over the covered headers and comparing the computed value to that contained in the ICV field of the AH header. Both the sender and receiver (the final destination in the case that a routing header is present) MUST independently and deterministically perform the same computation over the same data.

1.1 Handling mutable fields in AH

Certain fields may be modified during transit (i.e. mutable fields). To ensure that the sender and receiver both produce the same result in ICV computation for mutable fields, Section 5.3.3.1 of [RFC4302] specifies:

* If a field is mutable and its value at the (IPsec) receiver is not predictable, then the value of the field is set to zero for purposes of the ICV computation.

* If a field is mutable and its value at the (IPsec) receiver is predictable, then the predicted value is inserted into the field for purposes of the ICV computation.

1.2 Mutable fields in Segment Routing Header

Per [RFC8200] and [SRH], there are three instances of mutable fields related to segment routing:

* IPv6 destination address: The value of the destination address is predictable at the receiver. This is the last address in the segment routing list (destination address set when segments left goes to zero).

* Segments left: This is a field in the routing header and it’s value is predictable at the receiver. The field’s value is decremented at each intermediate destination such that the value at the final destination will be zero.

* Mutable SRH TLVs: Per [SRH], if the high order bit of an SRH TLV type is set then the TLV data for the corresponding TLV is mutable. The value of the TLV data for a mutable TLV is not predictable at the receiver.
2 Handling mutable SRH fields for ICV calculation

When performing the ICV calculation, at either the sender or receiver, the following values are set in the packet for the purpose of the calculation when an SRH header is present:

* The IPv6 destination address is set to final address in the segment routing list.

* Segments left field in the routing header is set to zero.

* For any SRH TLV whose high order bit is set, set the corresponding TLV data to all zeroes.

In pseudo code this is:

```c
/* opt is a char pointer to the segment routing header, */
/* iph is a pointer to the IP header of the packet */

/* Set segments left to zero */
if (opt[3] != 0) {
    opt[3] = 0
    /* Set destination to final address */
    iph->dest_address = *(struct ipv6_address *)&opt[8]
}

/* Determine offset of TLVs */
off = 8 + (opt[4] << 4)
len = ((opt[1] + 1) << 3) - off

/* Zero data for mutable TLVs */
while (len > 0) {
    if (opt[off] == 0) {
        optlen = 1
    } else {
        if (opt[off] & 0x80)
            memset(&opt[off + 2], 0, opt[off + 1])
        optlen = opt[off + 1] + 2
    }
    off += optlen
    len -= optlen
}
3 Security Considerations

The subject of this document is security using Segment Routing Header with the Authentication Header.

4 IANA Considerations

There are no IANA considerations in this document.

5 References

5.1 Normative References


5.2 Informative References

Author’s Address

Tom Herbert
Quantonium
Santa Clara, CA
USA

Email: tom@quantonium.net