Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 16, 2012

F. Templin, Ed.
Boeing Research & Technology

January 13, 2012

The SEAL IPv6 Destination Option
draft-templin-sealopt-01.txt

Abstract

The Subnetwork Encapsulation and Adaptation Layer (SEAL) provides a mid-layer header designed for the encapsulation of an inner network layer packet within outer network layer headers. SEAL also supports a transport mode of operation, where the inner payload corresponds to an ordinary transport layer payload. However, SEAL can also provide benefit when used as an IPv6 destination option that contains a digital signature inserted by the source. The source can thereafter use the signature to verify that any ICMPv6 messages received actually came from a router on the path, while destinations that share a secret key with the source can verify the signature to ensure data origin authentication.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The Subnetwork Encapsulation and Adaptation Layer (SEAL) [I-D.templin-intarea-seal] provides a mid-layer encapsulation designed for the encapsulation of an inner network layer packet within outer network layer headers, i.e., in a very similar manner as for GRE [RFC1701] and IPsec AH [RFC4302]. SEAL also supports a transport mode of operation, where the encapsulated payload corresponds to an ordinary transport layer protocol payload.

However, SEAL can also provide benefit when used as an IPv6 destination option [RFC2460] that contains a digital signature inserted by the source. The source can thereafter use the signature to verify that any ICMPv6 messages [RFC4443] received actually came from a router on the path, while destinations that share a secret key with the source can verify the signature to ensure data origin authentication.

2. SEAL IPv6 Destination Option

The SEAL IPv6 destination option can be inserted in either a "short form" or a "long form". In short form, the option includes a digital signature. In long form the option also includes an Identification value useful for anti-replay sequencing. The short form is formatted as shown in Figure 1:

```
                                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                   |  Option Type  | Opt Data Len=4|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Signature                           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: SEAL IPv6 Destination Option Format - Short Form

Option Type (8) an 8-bit field that encodes the destination option code for SEAL, with the value '00' in the high-order two bits.

Option Data Length (8) an 8-bit length of the option data field measured in octets. Set to 4 in short format, and set to 8 in long format.

Digital Signature (32)
a 32-bit digital signature. When a cryptographic signature is used, covers the leading 128 bytes of the packet beginning with the destination option header (or up to the end of the packet). The value 128 is chosen so that at least the IPv6 extension headers and the leading portion of the inner packet are covered by

the signature.

The long form is formatted as shown in Figure 2

```
                                      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                      |  Option Type  | Opt Data Len=8|
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                           Signature                           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                        Identification                         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: SEAL IPv6 Destination Option Format - Long Form

Identification (32)

a 32-bit per-packet identification field. Set to a monotonically-incrementing 32-bit value for each packet transmitted, beginning with 0.

The IPv6 source inserts a SEAL destination option when it needs to ensure that any resulting ICMPv6 error messages came from a router on the path and not from an off-path attacker. When the source receives an ICMPv6 error message, it verifies that the signature is correct. When a cryptographic signature is used, the source calculates the signature over the leading 128 bytes of the packet based on a secret hashing algorithm of its choosing. The source should choose a hashing algorithm that would make it extremely difficult for an off-path attacker to guess.

The destination may or may not recognize the SEAL destination option. If the destination does not recognize the option, it skips the option and processes the next option. If the destination recognizes the option (and if the option contains a cryptographic signature), the destination may either verify or ignore the signature according to its configuration. If the destination is configured to verify the signature, then it should accept the packet if the signature is correct and discard the packet if the signature is incorrect.

3. IANA Considerations

The IANA is instructed to allocate an IPv6 destination option for SEAL, with the value '00' in the high-order two bits.

4. Security Considerations

The source can use the SEAL destination option to verify that ICMPv6 messages were delivered by an on-path router and not an off-path

attacker. The signature may also be useful for other authenticating purposes, e.g., if the destination shares a secret key with the source. The packet identification field may also be useful for anti-replay sequencing.

5. Acknowledgments

This work was motivated by recent discussions on the 6man mailing list, and build on earlier investigations with SEAL. Sreenatha Setty provided valuable comments that helped clarify aspects of the document.

6. References

6.1. Normative References

[I-D.templin-intarea-seal]
Templin, F., "The Subnetwork Encapsulation and Adaptation Layer (SEAL)", draft-templin-intarea-seal-42 (work in progress), December 2011.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

6.2. Informative References

[RFC1701] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

Author's Address

Fred L. Templin (editor)
Boeing Research & Technology
P.O. Box 3707
Seattle, WA 98124
USA

Email: fltemplin@acm.org