SFC Working Group
Internet-Draft
Intended status: Informational
Expires: July 24, 2016

T. Reddy
Cisco
D. Migault
Ericsson
C. Pignataro
P. Quinn
Cisco
C. Inacio
CERT/SEI/CMU

January 21, 2016

NSH Security and Privacy requirements
draft-reddy-sfc-nsh-security-req-00.txt

Abstract

This document defines Network Service Header (NSH) security and privacy requirements.

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 24, 2016.

Table of Contents

1. Introduction

Service function chaining (SFC) [RFC7665] involves steering traffic flows through a set of service functions in a specific order, such an ordered list of service functions is called a Service Function Chain (SFC). The actual forwarding path used to realize an SFC is called the Service Function Path (SFP). Network Service Headers (NSH) [I-D.ietf-sfc-nsh] provides a mechanism to carry metadata between service functions. The NSH structure is defined in [I-D.ietf-sfc-nsh] and NSH data can be divided into two parts:

- Path information used to construct the SFP such as the SFP ID and Service Index.

- Metadata carrying the information about the packets being chained.

Note that the payload encapsulated by NSH is not part of the NSH data.

This document defines security requirments for NSH data and privacy requirements for NSH metadata.

2. Requirements notation

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. NSH Security and Privacy Requirements

This section provides requirements and recommendation for the SFC Data Plane.

REQ1: In a SFC domain where attackers can modify NSH data or generate spoofed NSH data, NSH data MUST be authenticated and integrity protected.

REQ2: In a SFC domain where attackers can capture and replay NSH data, NSH data MUST provide a mechanism for replay detection and replay prevention mechanism MUST be enforced by the SF component processing the NSH data.

REQ3: In a SFC domain where attackers can modify the NSH encapsulated packet, NSH encapsulated packet MUST be authenticated and integrity protected.

REQ4: In a SFC domain where pervasive monitoring [RFC7258] is possible, NSH metadata MUST be encrypted and MUST NOT reveal privacy sensitive metadata to attackers. Privacy specific threats are discussed in Section 5.2 of [RFC6973].

REQ5: TBD: To avoid fragmentation and amplification attacks, NSH data MUST be kept under Maximum Transmission Unit (MTU) including the byte overhead of the encapsulated packet.

REQ6: Negotiation of authentication, message integrity protection and encryption algorithms between SF components MUST be capable of detecting downgrade attacks.

REQ7: No device other than the SF components in the SFP SHOULD be able to update the integrity protected NSH data. SF components not in the SFP SHOULD NOT hold the keying material to act on the NSH data.

REQ8: No device other than the SF components in the SFP SHOULD be able to decrypt and update the NSH metadata. SF components not in the SFP SHOULD NOT hold the keying material to decrypt the NSH metadata.

4. IANA Considerations

None.

5. Security Considerations

NSH data is at risk from four primary attacks:

- A man-in-the middle attacker modifying NSH data.
- Attacker spoofing NSH data.
- Attacker capturing and replaying NSH data.
- NSH metadata revealing privacy sensitive information to attackers.

In a SFC domain where all the above attacks are possible, NSH data MUST be authenticated, integrity protected, replay protection MUST be supported and NSH metadata MUST be encrypted for confidentiality.

6. Acknowledgments

TODO

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

7.2. Informative References

[I-D.ietf-sfc-nsh] Quinn, P. and U. Elzur, "Network Service Header", draft-ietf-sfc-nsh-01 (work in progress), July 2015.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <http://www.rfc-editor.org/info/rfc7665>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

Authors' Addresses

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Bangalore, Karnataka 560103
India

Phone: +91 9886
Email: tireddy@cisco.com

Daniel Migault
Ericsson
8400 boulevard Decarie
Montreal, QC H4P 2N2
Canada

Phone: +1 514-452-2160
Email: daniel.migault@ericsson.com

Carlos Pignataro
Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
USA

Phone: +1 919-392-7428
Email: cpignata@cisco.com

Paul Quinn
Cisco Systems, Inc.

Email: paulq@cisco.com

Christopher Inacio
CERT, Software Engineering Institute, Carnegie Mellon University
4500 5th Ave
Pittsburgh, PA 15213
USA

Phone: +1 412-268-3098
Email: inacio@cert.org