Network Working Group
Internet Draft
Intended status: Standards Track
Expires: April 20, 2024

Y. Liu
S. Zhang
China Unicom
C. Lin
M. Chen
New H3C Technologies

October 23, 2023

Application-aware Networking (APN6) Header Authentication
draft-liu-apn-header-auth-00

Abstract

This document proposes an authentication method to verify the application-aware networking (APN) header.

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), 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/ietf/1id-abstracts.txt

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

This Internet-Draft will expire on April 20, 2024.

Table of Contents

1. Introduction

Application-aware Networking (APN) conveys an attribute along with data packets into the network and make the network aware of data flow requirements at different granularity levels [I-D.li-apn-problem-statement-usecases]. Such an attribute is encapsulated in the packets, and used by various nodes/service functions along the path to provide corresponding services. [I-D.li-apn-header] defines the APN header which can be used in different data planes to carry the APN attribute.

As shown in Figure 1, an APN header carried in the data packet may traverse multiple domains, and forwarded by using different traffic engineering technologies in each domain to guarantee SLA. So, the ingress edge device in each domain needs to check the APN header and determine the policy to be applied in that domain. A malicious attack through the APN header can cause packets to be forwarded incorrectly or occupy incorrect resources.

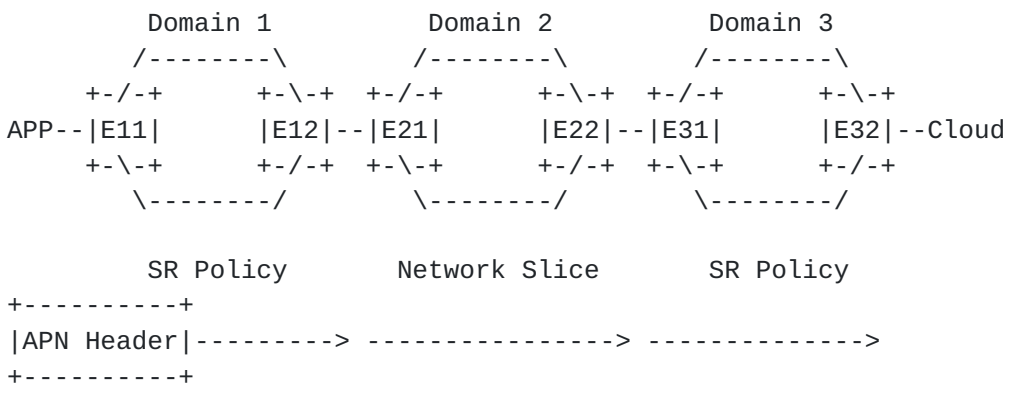


Figure 1: An Example of APN

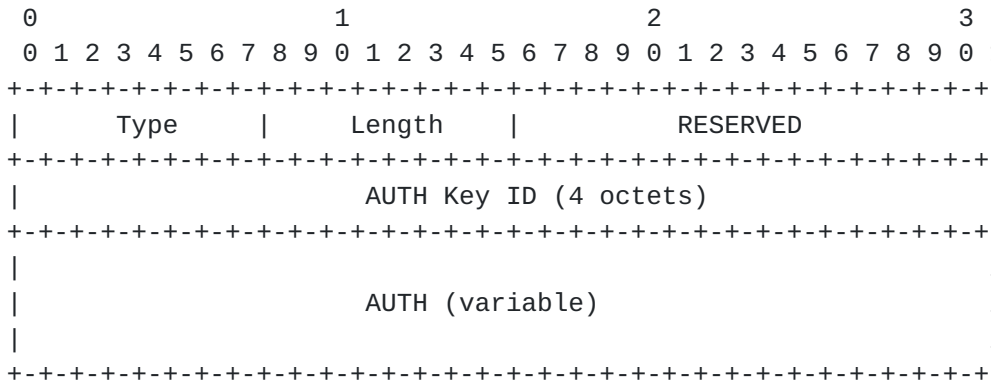
This document proposes an authentication method to verify the APN header, which can prevent the malicious attack through the APN header. The APN Authentication TLV and its encapsulation on IPv6 data plane are defined.

1.1. Requirements Language

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. APN Authentication TLV

The APN Authentication TLV is defined in this document to authenticate the APN header. The TLV has the following format:



o Type: TBD.

o Length: 1 octet. The length value is variable.

- RESERVED: 16 bits. MUST be 0 on transmission.

- AUTH Key ID: A 4-octet opaque number that uniquely identifies the hash algorithm, signature algorithm, and certificate serial number used for signature authentication.

- AUTH: Signature authentication, in multiples of 8 octets, at most 32 octets.

The APN Authentication TLV may be carried within the APN Header or carried after the APN Header, as shown in Figure 2. It depends on the format and data plane encapsulation of APN Header.

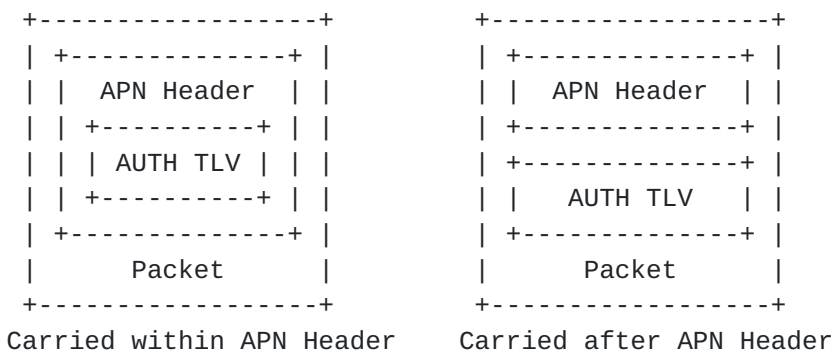


Figure 2: Encapsulation of APN Authentication TLV

3. Encapsulation on IPv6 Data Plane

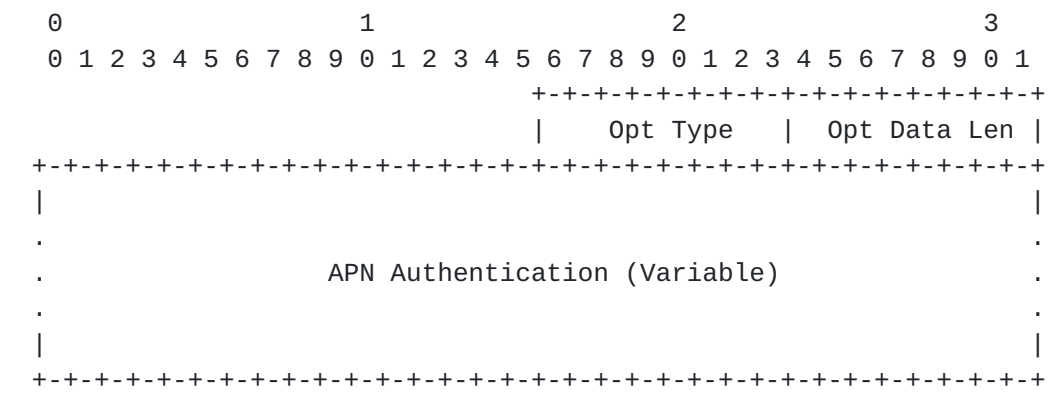
[I-D.li-apn-ipv6-encap] defines the encapsulation of the APN header on IPv6 data plane. Correspondingly, this document defines the encapsulation of the APN Authentication TLV on IPv6 data plane.

The encapsulation defined in this section carries the APN Authentication TLV after the APN Header.

3.1. The APN Authentication Option

An IPv6 Header option [RFC8200], the APN Authentication option, is defined.

The APN Authentication option can be carried in IPv6 Hop-by-Hop Options Header (HBH) and IPv6 Destination Options Header (DOH).



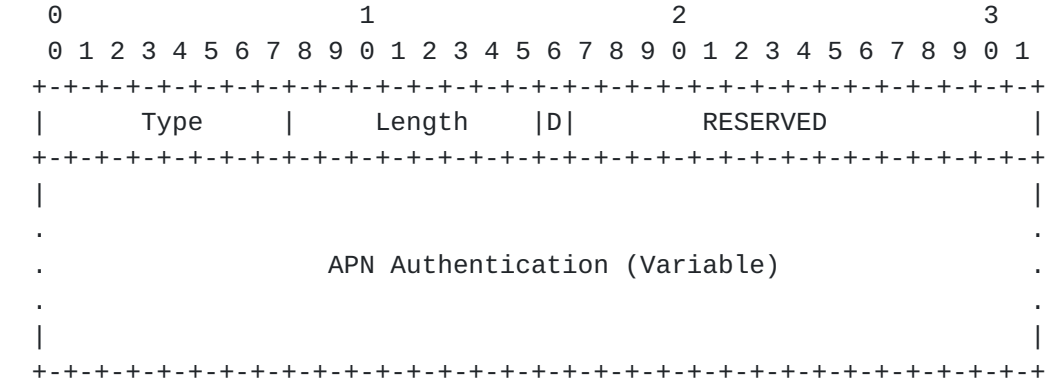
o Opt Type: TBD.

o Opt Data Len: An 8-bit unsigned integer. Length of the Option Data field of this option, that is, length of the APN Authentication TLV.

o APN Authentication: It carries the APN Authentication TLV as specified in Section 2.

3.2. The APN Authentication SRH TLV

An SRH TLV [RFC8754], the APN Authentication SRH TLV, is defined. The APN Authentication SRH TLV is OPTIONAL and has the following format:



o Type: TBD2.

o Length: The length of the variable length data in bytes.

o D: 1 bit. When it is set, it indicates the Destination Address verification is disabled due to use of a reduced segment list.

o RESERVED: 15 bits. MUST be 0 on transmission and ignored on receipt.

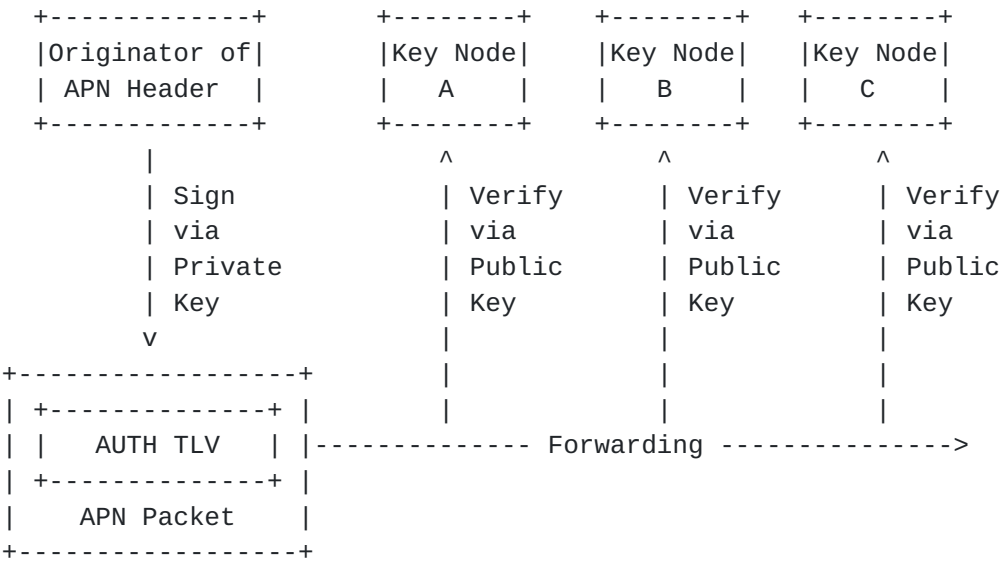
o APN Authentication: It carries the APN Authentication TLV as specified in Section 2.

4. Procedure

The authentication of the APN header applies asymmetric cryptography and hash-based signature.

The originator of APN (e.g. application client or APN ingress edge device) generates the signature by using the private key, the hash algorithm and the asymmetric algorithm. Then it encapsulates and forwards the APN packet with the APN Authentication TLV.

Signature verification is required at key network nodes (e.g. ingress edge device of each domain along the forwarding path). The hash value is calculated using the same hash algorithm. The signature in the APN Authentication TLV is decrypted using the public key and the same asymmetric algorithm. Then the decryption result is compared with the hash value to verify the APN header.



The management of asymmetric keys is out of scope in this document.

4.1. Signing and Verification on IPv6 Data Plane

On IPv6 data plane, a concatenation of the following fields from the IPv6 header and the APN header is used to calculate hash value for signing and verification:

o IPv6 header: Source address (16 octets)

- IPv6 header: Destination address (16 octets)
- APN header: APN-ID-Type (1 octet)
- APN header: APN-Para-Type (2 octets)
- APN header: APN-ID (4, 8, or 16 octets, according to APN-ID-Type)

5. Security Considerations

TBD.

6. IANA Considerations

TBD.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

7.2. Informational References

[I-D.li-apn-problem-statement-usecases] Li, Z., Peng, S., Voyer, D., Xie, C., Liu, P., Qin, Z., and G. S. Mishra, "Problem Statement and Use Cases of Application-aware Networking (APN)", Work in Progress, Internet-Draft, draft-li-apn-problem-statement-usecases-08, 3 April 2023, <https://datatracker.ietf.org/doc/html/draft-li-apn-problem-statement-usecases-08>.

[I-D.li-apn-header] Li, Z., Peng, S., and S. Zhang, "Application-aware Networking (APN) Header", Work in Progress, Internet-Draft, draft-li-apn-header-04, 12 April 2023, <https://datatracker.ietf.org/doc/html/draft-li-apn-header-04>.

[I-D.li-apn-ipv6-encap] Li, Z., Peng, S., and S. Zhang, "Application-aware IPv6 Networking (APN6) Encapsulation", Work in Progress, Internet-Draft, draft-li-apn-ipv6-encap-07, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-li-apn-ipv6-encap-07>.

Authors' Addresses

Ying Liu
China Unicom
China
Email: liuy619@chinaunicom.cn

Shuai Zhang
China Unicom
China
Email: zhangs366@chinaunicom.cn

Changwang Lin
New H3C Technologies
China
Email: linchangwang.04414@h3c.com

Mengxiao Chen
New H3C Technologies
China
Email: chen.mengxiao@h3c.com