IPv6 Extension Header (Performance and Diagnostic Metrics (PDM) Destination Option)
draft-ietf-ippm-encrypted-pdmv2-01

IETF114

N. Elkins: Inside Products, Inc.
M. Ackermann: BCBS Michigan
A. Deshpande: NITK Surathkal
T. Pecorella, A. Rashid: University of Florence
Brief explanation of PDM

• RFC8250: IPv6 Performance and Diagnostic Metrics (PDM) Destination Option

• To assess performance problems, this document describes optional headers embedded in each packet that provide sequence numbers and timing information as a basis for measurements. Such measurements may be interpreted in real time or after the fact. This document specifies the Performance and Diagnostic Metrics (PDM) Destination Options header.

• PDMv2: encrypts PDM
Status

• Early SECDIR review

• Continuing work on implementation

• Testing of extension headers across the Internet
SECDIR Review

I'm saying the draft is not yet ready primarily because it's early, and there is a "TBD" in "5.3 Security Goals for Authentication". That said, I'm not sure there's much to add here beyond the communicating parties being mutually authenticated.

The security considerations section addresses authentication by stating, "the Authentication and Authorization of Clients and Servers is thus delegated to the respective Organizations." I would add that the selected encryption scheme (HPKE incorporating KEM, KDF, and AEAD) should cover this requirement.

I'll also mention that authentication is mentioned in 5.3 but seemingly ignored in the list of things PDMv3 DOH needs to consider (see the middle of page 12).

Otherwise, the security considerations section covers the relevant threat scenarios reasonably well, and the document seems to provide a methodology to provide delegated trust, as claimed.
Can IPv6 Extension Headers Be Used on the Internet?

• Controversy for many years

• A number of studies showing that IPv6 extension headers get dropped at very high percentage rates.

• Studies (by and large) sent “Test” IPv6 extension headers to Alexa top n sites

• If this is true, our work on our IPv6 Extension Header Destination Option Performance and Diagnostic Metrics (PDM) is really for naught
What we did

• Used a small hosting service (not one of the “brand-name” ones)
• Using real PDM data, in DOH EHs, on actual applications sessions (FTP, HTTP, etc)
• Locations throughout the world
• *Using a kernel patch in FreeBSD to install PDM*

1. PDM-Warsaw
2. PDM-Toronto
3. PDM-Seattle
4. PDM-Mumbai
5. PDM-Melbourne
6. PDM-Frankfurt

All machines are FreeBSD with a modification to the kernel to send PDM IPv6 Destination option with every packet
Tested large FTP: Toronto to Mumbai (with PDM)

- 220-------- Welcome to Pure-FTPd [privsep] [TLS] --------
- 220-You are user number 1 of 50 allowed.
- 220 You will be disconnected after 15 minutes of inactivity.
- 331 User PDMuser OK. Password required
- 230 OK. Current directory is /
- Remote system type is UNIX.
- Using binary mode to transfer files.

- 229 Extended Passive mode OK (|||3353|)
- 150-Accepted data connection
- 150 27872.0 kbytes to download
- 100%
  |****************************************************************|
  | 27872 KiB  222.31 KiB/s   00:00 ETA
- 226-File successfully transferred
- 226 125.107 seconds (measured here), 222.78 Kbytes per second
- 28540928 bytes received in 02:05 (222.31 KiB/s)
- 221-Goodbye. You uploaded 0 and downloaded 27872 kbytes.
- 221 Logout.
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>PSN This Packet</th>
<th>PSN Last Received</th>
<th>Info</th>
</tr>
</thead>
</table>

**PDM IPv6 Extension Header**

**Destination Option**
Showing both Extension Headers

**Destination Options for IPv6**
- Next Header: Fragment Header for IPv6 (44)
  - Length: 1
  - [Length: 16 bytes]
- Performance and Diagnostic Metrics
  - Type: Performance and Diagnostic Metrics (0x0f)
    - Length: 10
    - Scale DTLR: 34
    - Scale DTLS: 42
    - PSN This Packet: 23912
    - PSN Last Received: 20490
    - Delta Time Last Received: 37754
    - Delta Time Last Sent: 45216
- PadN
  - Type: PadN (0x01)
    - Length: 0
    - PadN: <none>
- Fragment Header for IPv6
  - Next header: TCP (6)
  - Reserved octet: 0x00
  - 0000 0000 0000 0... - Offset: 0 (0 bytes)
  - .... .... .... .... - Reserved bits: 0
  - .... .... .... ....1 = More Fragments: Yes
  - Identification: 0x73059a89
  - [Reassembled IPv6 in frame: 52]
  - Data (1432 bytes)
Bottom line

1. PDM-FTP Toronto to Warsaw - worked
2. PDM-FTP Toronto to Seattle - worked
3. PDM-FTP Toronto to Mumbai - worked
4. PDM-FTP Toronto to Melbourne - worked
5. PDM-FTP Toronto to Frankfurt - worked

Traces available for all to look at.

Come to the Hackathon (or HackDemo) if you want to see for yourself.
### IETF Curl to Warsaw: Response

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Dest Port</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>553</td>
<td>11.457978</td>
<td>2001:67c:370:128:1d... 2a05:f480:2400:19d5...</td>
<td>TCP</td>
<td>74</td>
<td>80 50317 → 80 [ACK] Seq=1 Ack=1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>554</td>
<td>11.459505</td>
<td>2001:67c:370:128:1d... 2a05:f480:2400:19d5...</td>
<td>HTTP</td>
<td>666</td>
<td>80 GET / HTTP/1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>557</td>
<td>11.561527</td>
<td>2a05:f480:2400:19d5... 2001:67c:370:128:1d...</td>
<td>HTTP</td>
<td>316</td>
<td>50317 HTTP/1.1 304 Not Modified</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source Address: 2a05:f480:2400:19d5:5400:4ff:fe0f:8059

**Destination Options for IPv6**

- Next Header: TCP (6)
- Length: 1
  - [Length: 16 bytes]

**Performance and Diagnostic Metrics**

- Type: Performance and Diagnostic Metrics (0x0f)
- Length: 10
  - Scale DTLR: 0
  - Scale DTLS: 0
  - PSN This Packet: 45234
  - PSN Last Received: 0
  - Delta Time Last Received: 0
  - Delta Time Last Sent: 0
Next Time

• Continuing implementation

• Will have drafts at v6ops & IPPM on EH testing

• Working on EH BCP and other drafts

• Welcome collaborators
Questions?