encrypted IPv6 Performance and Diagnostic Metrics Version 2 (EPDMv2) Destination Option

draft-elkins-ippm-encrypted-pdmv2-00

Nalini Elkins: Inside Products: nalini.elkins@insidethestack.com
Michael Ackermann: BCBS Michigan: mackermann@bcbsm.com
Ameya Deshpande: NITK, Surathkal: ameyanrd@gmail.com
Tommaso Pecorella: University of Florence: tommaso.pecorella@unifi.it
Adnan Rashid: University of Florence: adnan.rashid@unifi.it
Setting the stage

• We need performance data

• Metadata can be misused

• We need encryption

• We propose a light-weight, scalable methodology

• Maybe can be used by: IOAM? other packet headers? IPv6 extension headers? PING? Traceroute?
PDM: Misuse

• Passive Attacks
  • Learn possible weak points
    • e.g., to launch a DoS attack,

• Active Attacks
  • Trigger inappropriate network management operations.
PDMv2 (How does it work? - Overview)

- PDMv2 provides an option for encrypted as well as unencrypted data flow.

For the encrypted flow:
- PDMv2 consists of a registration phase and data transfer.
- The registration phase consists of "SharedSecret" negotiation.
  - How will this negotiation take place?
  - What about the large enterprises having many servers and client?
- The registration phase is "one time" process done before PDM data transfer.
- In a PDM data flow, there will encryption-decryption and occasional KDF taking place.

For the unencrypted flow:
- Similar to PDM
PDMv2 Scenario and Secured paths

<table>
<thead>
<tr>
<th>Links</th>
<th>Entity-A</th>
<th>Entity-B</th>
<th>Security Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary (Writer) Client</td>
<td>Primary (Writer) Server</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Primary (Writer) Client &amp; Server</td>
<td>Secondary (Reader) Client / Server</td>
<td></td>
<td>&lt;tbd&gt;</td>
</tr>
<tr>
<td>Secondary (Reader) Client-N</td>
<td>Secondary (Reader) Server-N</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Why Primary Client / Primary Server Scenario?

- Enterprises typically have multiple servers and many, many clients
- These clients and servers may be in multiple locations
- It may be less overhead to have a secure location (ex. Shared database) for every server / client to share keys
- Otherwise, each client needs to keep track of the keys for each server
HPKE in PDMv2

1. Registration Phase
   • KEM -> Shared master secret

2. Online Phase -> Every $2^{15}$ packets
   • KDF -> Temporary Session Key
   • PRSEQ (Pseudo-random non-repeating sequence) -> Nonce
     • Runtime generation or pre-generation (tbd)

3. Online Phase -> Every packet
   • AEAD-> Encryption & Decryption
QUESTIONS ????????