Operational Implications of IPv6 Packets with Extension Headers
(draft-gont-v6ops-ipv6-ehs-packet-drops)

Fernando Gont
Nick Hilliard
Gert Doering
Will (Shucheng) Liu
Warren Kumari

IETF 94
Yokohama, Japan. November 1-6, 2015
Overview of this document

• Provides an overview of the operational and security implications of IPv6 EHs
• Documents why some operators intentionally drop packets that contain IPv6 EHs
• Relationship with draft-ietf-v6ops-ipv6-ehs-in-real-world:
  – Measured packet drops need not be intentional in all cases
  – This document summarizes the motivation for intentional packet drops
Security Implications of IPv6 EHs

• Evasion of security controls
• DoS due to processing requirements
• DoS due to implementation errors
• Extension Header-specific issues
Operational Implications (I)

- Some middleboxes and intermediate systems need to obtain layer-4 information.
- When they are unable to obtain that information, they may drop the corresponding packet.
- Requirement to process layer-4 information:
  - Enforcing infrastructure ACLs
  - DDoS Management and Customer Requests for Filtering
  - ECMP and Hash-based Load-Sharing
  - Packet Forwarding Engine Constraints
Operational Implications (II)

- Route-Processor Protection
  - In some implementations, processing the EH chain may punt the packet to a software path
  - HBH Options EH proves to be particularly challenging
Operational Implications (III)

- Inability to Perform Fine-grained Filtering
  - In some implementations, processing the EH chain may punt the packet to a software path
  - HBH Options EH proves to be particularly challenging
Moving Forward

• Adopt as WG document?