Hop-by-hop Options Extension Header

draft-ietf-6man-hbh-header-handling-04

Fred Baker
Ron Bonica
Current State of Affairs

• Network operators perceive the HBH Options Extension Header to be a DoS vector due to diversion of data processing to control path

• That perception justified (consistent with the specification)
  • Many implementations send every packet containing HBH to the control path
  • Even if the packet requires no processing (e.g., HBH contains only Pad Option)

• Therefore, many operators do one of the following
  • Discard all packets containing HBH
  • Forward all packets containing HBH without examining the HBH contents

• Therefore, HBH applicability is limited to controlled environments
  • Not the global Internet!
Desired State of Affairs

• Security vulnerabilities associated with HBH are mitigated to the greatest degree possible
  • Operators can control packet processing
  • HBH options not unnecessarily processed, or processed at wire speed

• Therefore, network operators do one of the following:
  • If they do not run any protocols that rely on HBH, routers forward packets containing HBH without examining HBH contents (data path)
  • If they run protocols requiring HBH, they examine and possibly process HBH contents (normally data path, but control path when intended to force that)
  • In neither case do they discard all packets containing HBH

• Therefore, HBH applicability is expanded
In other words...

• HBH option processing is no longer required in every router
  • Only among consenting adults

• When possible, HBH option processing is done inline in the data path.
Data Path Configuration Items

• List of recognized HBH Options
  • Default value: Empty
  • When the node is configured to support a protocol that relies on HBH, the list is augmented as required
  • Configuration may be automated (if a function is enabled that requires HBH, the corresponding HBH option is enabled as a side effect of configuration)
Updates to RFC 2460

• The first two bits of the HBH Option Type have no special meaning
  • E.g., the option type is now a 7 bit number
• Intermediate systems process only HBH options configured for.
Data Path Packet Processing

• RFC 7112: if the entire IPv6 header, including extensions, plus transport header is not in the first fragment,
  • Send an ICMP Parameter Problem to the packet source
  • Discard the packet

• Otherwise, if the list of recognized options is empty
  • Don’t even ask whether HBH Options Extension Header is present.
  • Forward as appropriate

• Otherwise, process recognized HBH Options in the order that they are listed
  • Ignore all unrecognized options
  • Sequentially process all recognized options
    • This may require the packet to be diverted to control path in control cases
  • Forward as appropriate
Result: Improved Applicability

• Today, HBH is applicable in extremely controlled environments
  • Not on the global Internet
  • Because on the global Internet, some intermediate nodes discard all packets containing HBH

• If the current proposal is widely deployed, protocols that rely on HBH will work better on the global Internet
  • Because network operators will not be motivated to discard all packets containing HBH
  • However, many intermediate nodes will ignore HBH

• So, some protocols that rely on HBH will work on the global Internet
  • But only if they don’t break when some intermediate nodes ignore HBH