Why Operators Filter Fragments and What It Implies

draft-taylor-v6ops-fragdrop-00

Joel Jaeggli <jjaeggli@zynga.com>
Lorenzo Colitti <lorenzo@google.com>
Warren Kumari <warren@kumari.net>
Eric Vyncke <evyncke@cisco.com>
Merike Kaeio <merike@doubleshotsecurity.com>
Tom Taylor <tom.taylor.stds@gmail.com>

The Perceived Problem

- Some operators filter IPv6 fragments (and ICMPv6 PTB)
  - makes applications relying on IPv6 fragmentation unreliable.
- More of a consideration the closer you are to the network edge.
- Motivations:
  - DoS potential (state consumption) introduced by fragments themselves
  - potential exploits taking advantage of inconsistent implementations
  - loss of performance due to slow-path processing of fragments
  - inability to apply stateless ACLs
  - requires fragment-specific load balancing strategy.
- Suggestion on the list that some of the dropping is due to implementation defaults, some is due to an overly-developed fear of information leakage.

Reactions On The List

- Ingress filtering at L4 used to minimize attack surface.
- Some operators would like IPv6 extension headers including fragment headers to go away, so ingress filtering at wire speed is easier.
  - broader issue.

Reactions On The List (cont'd)

- Less extreme view is to document the observance of the phenomenon, acknowledge what gets broken as a result, and perhaps provide advice that limits the scope of the damage.
- RFC 5722, RFC 6192, draft-ietf-6man-oversized-header-chain mentioned

Reactions On The List (cont'd)

“It's (probably ... until Fernando figures a way to hack it) safe to pass fragments without extension headers other than fragmentation header.

“It's also (probably) safe to drop non-initial fragments with extension headers (apart from the fragmentation header). If someone generates enough extension headers to overflow the minimum MTU, he has a problem anyway.”

-- Ivan Pepelnjak

Brian Carpenter counters: middleboxes need to be transparent to new extension headers to allow innovation. He agrees that long extension headers are not a good idea.

Summing Up

- Lots of other discussion, and some of the points can be brought out later
- The REAL questions:
  - can fragment dropping ever be justified?
  - If so, can the circumstances be spelled out carefully enough to be useful?
    - useful enough that operators refrain from dropping fragments unnecessarily
    - useful enough that originating hosts can predict whether fragments will be delivered reliably