Issues with Overlapping IPv6 Fragments

draft-krishnan-6man-overlap-fragment-01.txt

Suresh Krishnan

Issues with overlapping IPv4 fragments

- Overlapping fragments were allowed in the original IPv4 specification (RFC791)
- RFC1858 described an overlapping fragment attack that can be used to overwrite the TCP flags inside a packet
- This lead to the definition of a minimum fragment offset for fragments with non-zero offsets (minimum FO=2)
  - This ensures that the TCP flags from the initial fragment cannot be overwritten

Issues with overlapping IPv6 fragments

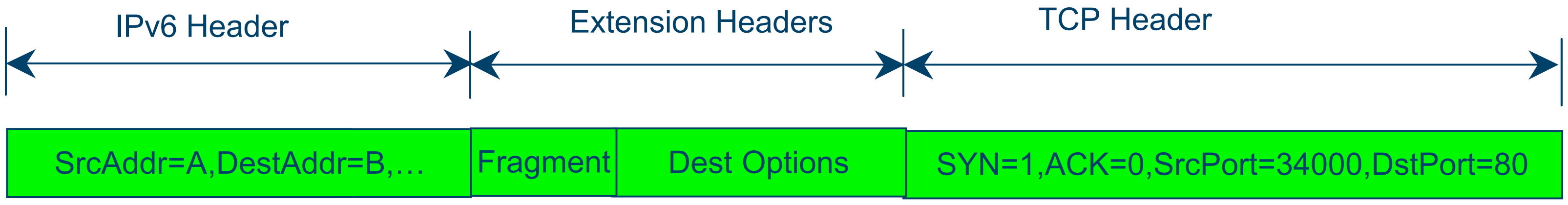
- Overlapping fragments are allowed by the fragmentation and reassembly algorithm specified in the current IPv6 base specification (RFC2460)
- The overlapping fragment attack described in RFC1858 is still applicable.
- This issue has been known for a while and has been documented in RFC4942 (IPv6 Transition/Co-existence Security Considerations)

What’s new?

- Scope of the attack has greatly increased
- Originally described issue only allows overwriting of TCP flags.
  - The main TCP header (with the ports) will always be in the first fragment
- IPv6 datagrams can include a destination options header
  - This header belongs to the fragmentable part of the datagram
- TCP header can be much further into the fragmentable part
  - Makes it possible to even overwrite port info.

Description of attack

Fragment 1



IPv6 Header

Extension Headers

TCP Header

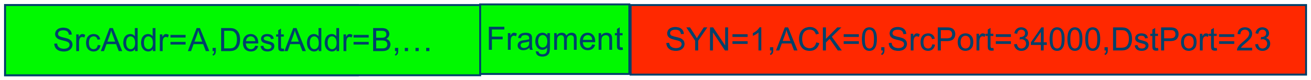
SrcAddr=A,DestAddr=B,…

Fragment

Dest Options

SYN=1,ACK=0,SrcPort=34000,DstPort=80

Fragment 2

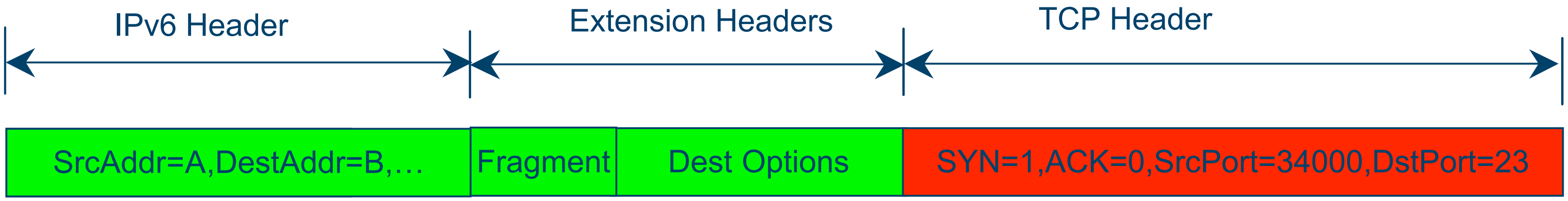


SrcAddr=A,DestAddr=B,…

Fragment

SYN=1,ACK=0,SrcPort=34000,DstPort=23

Reassembled Packet



IPv6 Header

Extension Headers

TCP Header

SrcAddr=A,DestAddr=B,…

Fragment

Dest Options

SYN=1,ACK=0,SrcPort=34000,DstPort=23

Recommended action

- Disallow overlapping fragments in IPv6
- Recommend existing implementations to fix this issue

Thanks

Questions?