Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/ICMPv6 Error Messages (draft-gont-opsec-icmp-ingress-filtering-02)

Fernando Gont
Ray Hunter
Jeroen Massar
Will Liu

IETF 99
Prague, Czech Republic. July 16-21, 2017
Goal

- Specify filtering policy to mitigate attacks based on spoofed ICMPv6 errors
  - Spoofed ICMPv6 PTB to play with PMTUD or trigger fragmentation
  - Spoofed ICMPv6 errors that might reset connections
  - etc.
- Should be deployed close to users (e.g. CPEs)
- Must never be applied in multihomed scenarios
Background on ICMP Error Generation

Packet (Src A, Dst D)

ICMP error
(Src B, Dst A)

ICMP error

Src Addr: B  Dst Addr: A
Src Addr: A  Dst Addr: D
ICMP-based Attack Scenario
IF embedded packet's Destination Address is from within my network
    THEN forward as appropriate

IF embedded packet's Destination Address is anything else
    THEN deny packet
Changes in version -03

- Change all IPv4 examples to IPv6 examples
- Explain possible limitations in inspecting ICMP payloads
- Include discussion of ICMP extension objects (RFC4884)
Moving forward

- Adopt as opsec wg item?