Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/ICMPv6 Error Messages

(draft-gont-opsec-icmp-ingress-filtering-01)

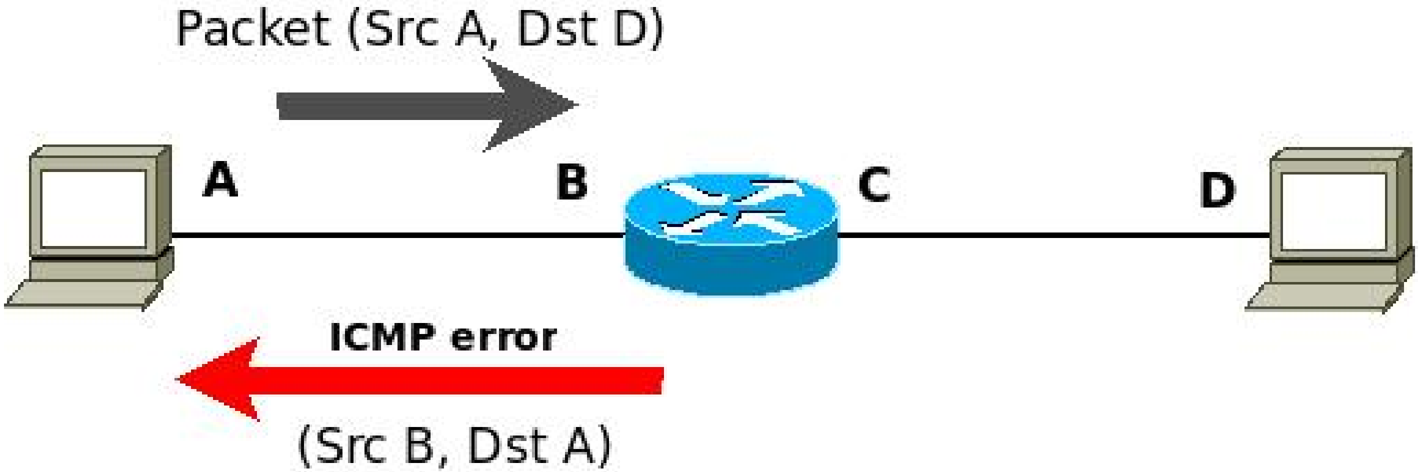
Fernando Gont
Ray Hunter
Jeroen Massar
Will Liu

IETF 92
Dallas, Texas, U.S.A. March 22-27, 2015

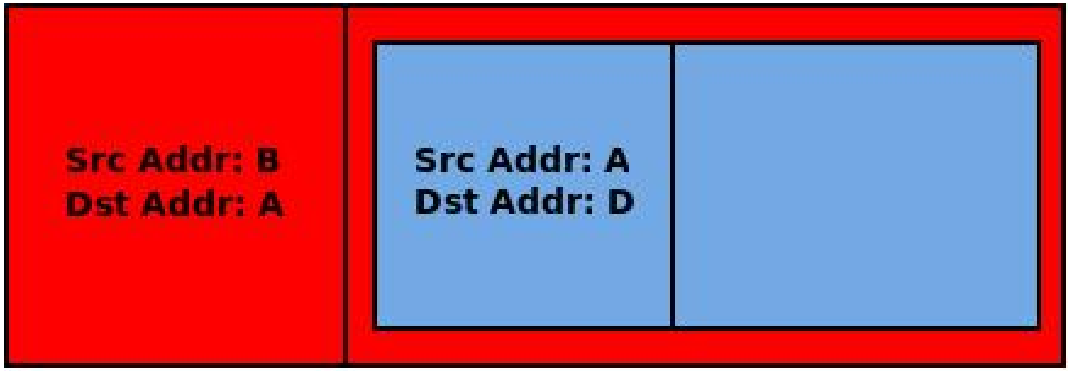
Background

- BCP38 mitigates network attacks that rely on IP source address spoofing
- However, BCP38 does not address ICMP-based attacks
  - in which the IP addresses of the **embedded packet** are spoofed

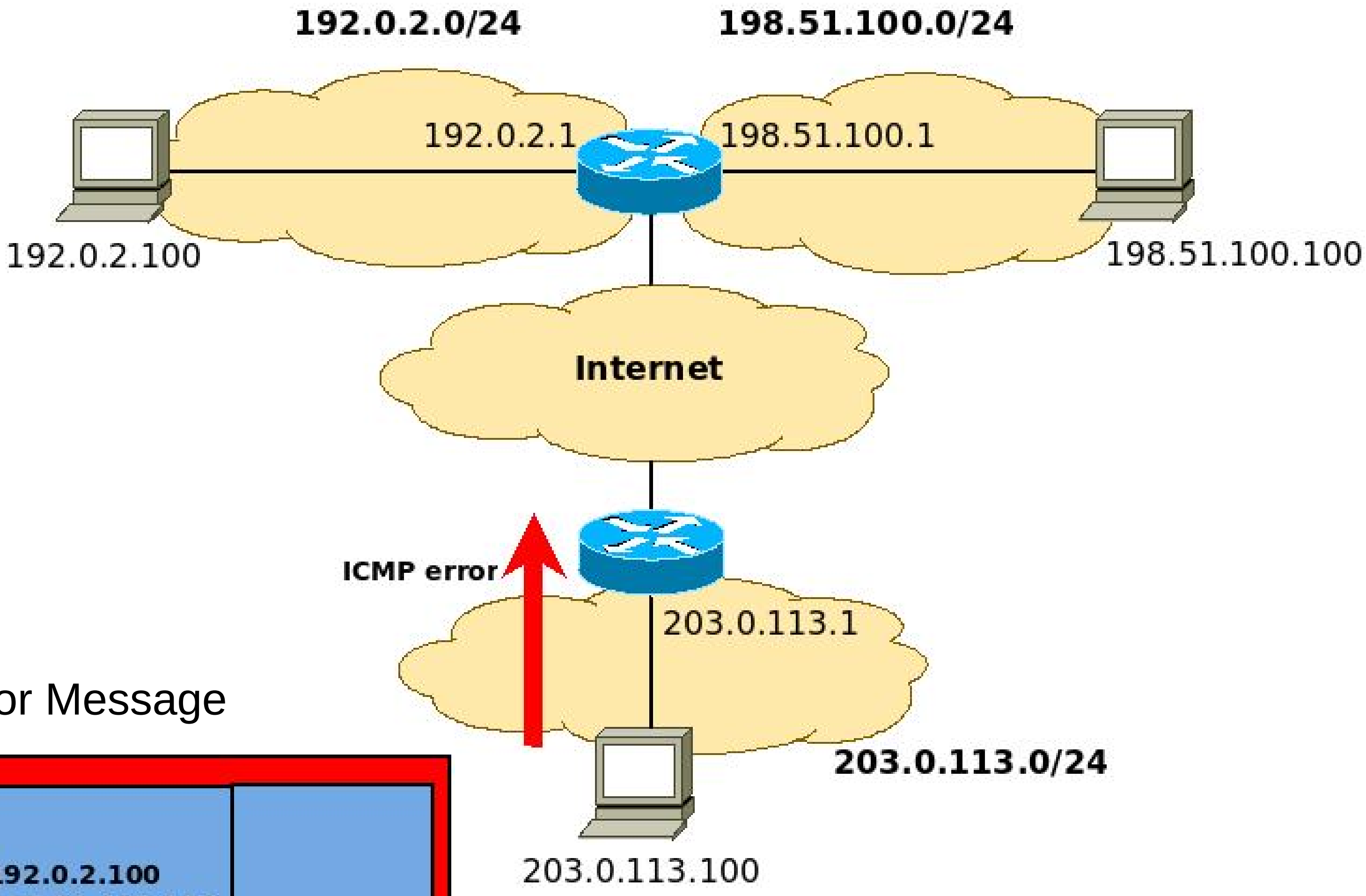
ICMP Generation



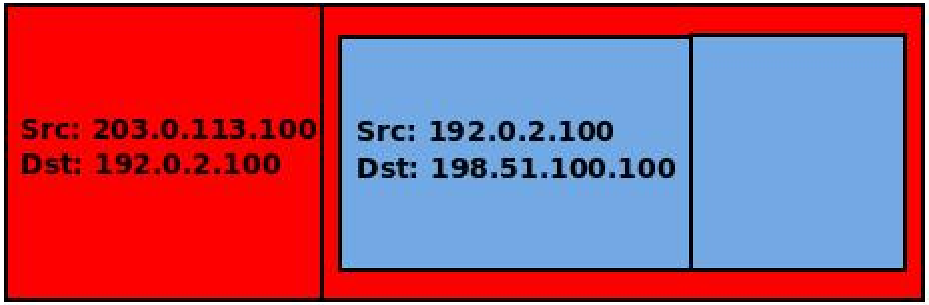
ICMP error



ICMP-based Attack Scenario



ICMP Error Message



Src: 203.0.113.100
Dst: 192.0.2.100

Src: 192.0.2.100
Dst: 198.51.100.100

draft-gont-opsec-icmp-ingress-filtering

- Simple, effective, and straightforward method for using ingress traffic filtering to mitigate attacks that use forged addresses in ICMP messages
- In-line with BCP38

draft-gont-opsec-icmp-ingress-filtering

- If implemented with ACLs:
  - 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
- **Or** perform unicast Reverse Path Forwarding (uRPF) on the Dst address of the embedded payload

Moving forward

- Adopt as opsec wg item?