BCOP on Anti-Spoofing

- Long known problem
- Deployment status
- Reason for this work
- Where more input needed

Lots of Advice re Anti-Spoofing

- BCP38 (RFC2827) was standardized in May 2000
  - Network Ingress Filtering: Defeating DoS Attacks Which Employ IP Source Address Spoofing
  - http://tools.ietf.org/html/bcp38
- BCP84 (RFC3704) was standardized in March 2004
  - Ingress Filtering for Multihomed networks
  - http://tools.ietf.org/html/bcp84
- Expired draft on deployment experiences
  - Experiences from Using Unicast RPF
  - Draft-savola-bcp84-urpf-experiences-03.txt

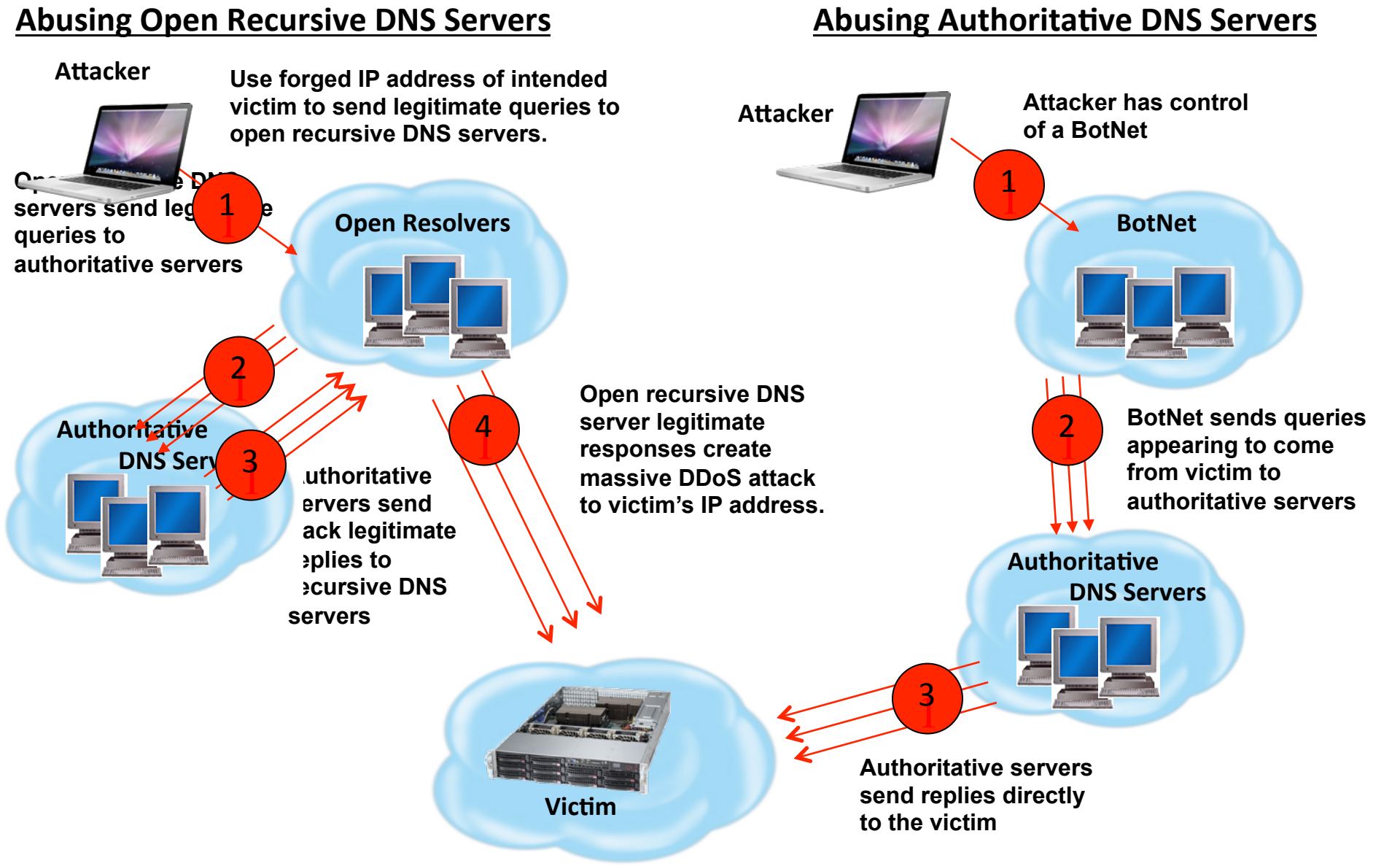
And there's more advice….

- ICANN Security and Stability Advisory Committee (SSAC) Documents
  - SAC004 – Securing the Edge (Oct 2002)
    - https://www.icann.org/en/system/files/files/sac-004-en.pdf
  - SAC065 – Advisory on Ddos Attacks Leveraging DDoS Infrastructure (Feb 2014)
    - https://www.icann.org/en/system/files/files/sac-065-en.pdf

Deployment Status

- Hard to definitively measure
  - http://spoofer.cmand.org
  - Others?
- Know this is still problem due to ongoing attacks
  - DNS, SNMP, NTP, etc
  - Amplification Hell
    - http://www.christian-rossow.de/articles/Amplification_DDoS.php

DNS Amplification Attacks Utilizing Forged (Spoofed) IP Addresses

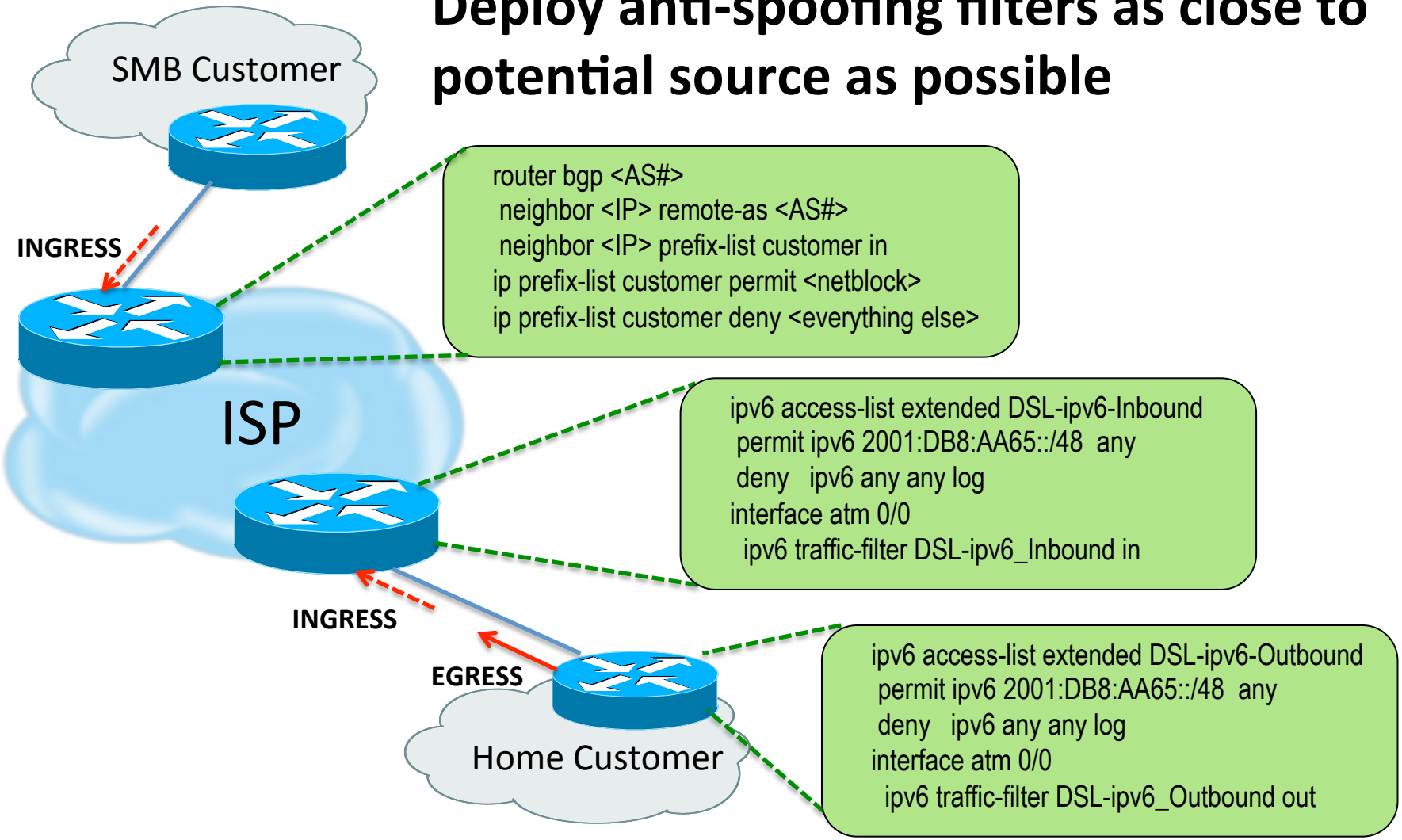


What's Goal In This Work

- Many documents tell you WHAT to do
- Few documents tell you HOW to do it
  - RIPE Anti-Spoofing Task Force How-To (May 2008)
    - http://www.ripe.net/ripe/docs/ripe-431
  - bcp38.info (ongoing)
- Not much information exists on vendor bugs and workarounds
- Not much information exists on practical use cases

Where Provide Anti-Spoofing?

Deploy anti-spoofing filters as close to potential source as possible



Where Input Needed

- How you implement anti-spoofing mechanisms?
  - Packet filters vs uRPF vs route filters vs ??
- Why are you not implementing anti-spoof mechanisms?
- What bugs have you run into?
- IXPs, ISPs
- Also Enterprises

How to get involved

- **Merike+bcop@doubleshotsecurity.com**
- **List coming soon**
- **Draft ETA End of November.**