Topic

DNS As Abused
Spoofed Source Attacks

- **attacker**
  - Src addr: (target)
- **Botted server, in the cloud, Gigabit speed**
- **Internet**
  - Dst addr: (target)
- **reflector**
- **target**
Securing the Edge

3.1. The typical vector for DDoS launches is a personal computer (PC) running operating system and application software that purposely trades off security for convenience. These computers are usually poorly managed, such that there are weak passwords or no passwords, known security "holes" that are never patched or closed, and services offered to the global Internet that the owner has no knowledge and no use for.

3.2. From the point of view of almost any single purveyor -- or consumer -- of operating system and application software, convenience will almost always have more perceived value than security. It is only when viewed in the aggregate that the value of security becomes obviously higher than the value of convenience.

3.3. With the advent of high speed "always on" connections, these PCs add up to either an enormous global threat, or a bonanza of freely retargetable resources, depending upon one's point of view.
DNS Response Rate Limiting (RRL)

• If you run a DNS content (“authority”) server, it has to be massively overprovisioned
• Because OPN’s don’t have SAV, your server is a purpose-built DNS DDoS reflecting amplifier
• BIND, NSD, Knot now support DNS RRL, which accurately guesses what’s safe to drop
• Your authority servers need this, whereas your recursive servers need to be firewalled off
RRL In Action: Afilias