Defense Strategies for DDoS Attacks

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb

A *Real* Network Security Issue

- Most "network security" problems are nothing of the sort.
- They're host vulnerabilities; the network is just an access vehicle.
  - Without the net, could a local user exploit the hole?
- DDoS *is* the network's problem.

Implications

- Host vendors can't fix it.
- Firewalls can't stop it.
- It's a network problem; the response must come from the network.

Response Classes

- Packet authentication
  - Find out who is sending the packets
- “Flow” identification
  - If we can identify it, can we control it?
  - Can we withhold authorization?

Packet Identification: Filtering

- Block packets with forged source address.
- Identifies site (and maybe LAN) that stuff is coming from.
- Granularity of filter is an issue.
- Can anyone cope with knowing 1000 attacking sites?

Source Identification Schemes

- Have network elements -- routers, switches, etc. -- identify packets of interest.
- Packet-marking -- set bits in packet header
- Logging -- notify NOC
- Tracers -- send extra packets to destination, identifying path

Prevention

- Must rate-limit “evil” packets.
  - But no “evil” bit in the header...
- Could try to limit all packets, but the Internet isn’t built that way.
- Possibility: limit packets towards victim, from high-bandwidth predecessor.
- Apply algorithm recursively.

Router Pushback

- Use existing mechanisms to find ill-behaving traffic towards some destination.
- Identify previous router hops for such traffic; tell them to rate-limit packets to your for that destination.
- If they're dropping packets, they tell their upstream neighbors.
- Note: pushback eventually shows traffic source.