Backbone Perspective

Ryan McDowell
ryanm@puck.nether.net
3/9/06

Agenda

- Things to keep in mind about backbone providers
- What unwanted traffic means to the backbone provider
- What's being attacked
- The reality of fighting unwanted traffic

Things to keep in mind about backbone providers

- IP Transit is a commodity
- Controlling cost is the only way to be profitable
  - Providers don't spend money on anything that doesn't have a positive ROI and a short payback period
    - Security, travel, conferences, salaries, DNS servers, etc
- There is a lot of old hardware in the network
  - It probably isn't going anywhere anytime soon (see above)
- NOC's are over worked and under paid (see above)
  - NOC's always have more tickets in the queue
  - NOC's are measured on MTTF/MTTR
    - Motivated to close the ticket as quickly as possible and move on to the next
  - It's difficult to keep highly skilled employees

Things to keep in mind about backbone providers

- They do not own the end hosts
- Providers are not going to publicly reveal how frequently their infrastructure is impacted
- They are large organizations and politics and organizational dynamics often prevent the right thing from being done

What unwanted traffic means to the backbone

- To the backbone provider, unwanted traffic means anything that impacts availability (their ability to deliver bits) or otherwise impacts their revenue
  - Infrastructure DoS attacks
  - Collateral damage from DoS that impacts more than one customer
  - Having a bad reputation (ie SPAM friendly, phishing hoster, etc)
- Everything else is not their problem and official resources will not be used

What's being attacked

- Core routers are not being directly attacked (yet)
  - Little financial incentive for the miscreants to do this right now
- Core links are usually not impacted
  - As long as attacks do not coincide with a fiber cut, there is ample capacity
- Customer/Peering edge often saturated
- Access router uplinks often saturated
- Access routers are directly attacked
  - SSH, IKE, RSH, SNMP, ICMP, Fragments, etc
- Service (such as DNS) are targeted

What's being attacked

- BGP hijacking
  - Intentional hijacking is usually for SPAMing
    - Meant to not draw attention
  - Fat finger attack is usually the culprit for noticeable hijacking events
- Worms
  - Impact the network, but not how you think
  - High pps, low bps
    - Core links not saturated
  - Indirect impacts are the problem
    - Multicast destination => MSDP SA storms
    - Edge link saturation => BGP instability

What's being attacked

- Spoofed versus non-spoofed
  - Some reports of a slight decline of spoofed attacks
    - Due to unicast reverse path forwarding/cable source verify dhcp?
  - Who cares if you have 10,000's bots…
- Majority of attacks still seems to be TCP/SYN, UDP flood
- However, more intelligent attacks are emerging
  - Application aware attacks
  - Reflection/amplification attacks (smurf^2)

The reality of fighting unwanted traffic

- The problem:
  - Number of (d)DoS related tickets: 100's per year
  - Number of actual significant (d)DoS events: 1000's per year
  - MTTR/MTTF for (d)DoS tickets is significantly higher than the average
- Question: Why should I work tickets that take a huge amount of effort, require my super NOC engineers to resolve, and increase my MTTR/MTTF if customers aren't complaining to the point of impacting revenue?
- Current answer: The "super" NOC engineers are dealing with the problem on their own time and dime
  - Working issues 24x7, just look at nsp-security
  - Fighting unwanted traffic is often a skunk works project
  - This is starting to change as more important services such as voice, video, circuit emulation, ATM/FR replacement (2547 VPN) is transported over the IP network

The reality of fighting unwanted traffic

- The reaction to unwanted traffic:
  - Requires a high level of skill
  - Is labor intensive
  - Is time consuming
  - Often has the potential to cause more problems than the unwanted traffic
  - Often blocks the good traffic with the bad
    - Protect the network by black holing the target
  - Is often a one-up in an arms race with the miscreants that we cannot win in the long term
    - (d)DoS mitigation appliances => better, application aware, bots and more devious reflection attacks
    - Deep packet inspection => XoHTTPS
  - Solutions often require universal deployment to be effective
  - Solutions often require capital expenditures to deploy