How Come We Have DDoS?

- Natural consequence of the way Internet is organized
  - Best effort service means routers don’t do much processing per packet and store no state – they will let anything through
  - End to end paradigm means routers will enforce no security or authentication – they will let anything through
- It works real well when both parties play fair
- It creates opportunity for DDoS when one party cheats
There Are Still No Strong Defenses Against DDoS

- You can make yourself harder to attack
- But you can’t make it impossible
- And, if you haven’t made it hard enough, there’s not much you can do when you are attacked
  - There are no patches to apply
  - There is no switch to turn
  - There might be no filtering rule to apply
  - Grin and bear it
Why Is DDoS Hard to Solve?

1. A simple form of attack
2. Designed to prey on the Internet’s strengths
3. Easy availability of attack machines
4. Attack can look like normal traffic
5. Lack of Internet enforcement tools
6. Hard to get cooperation from others
7. Effective solutions hard to deploy
1. Simplicity Of Attack

- Basically, just send someone a lot of traffic
- More complicated versions can add refinements, but that’s the crux of it
- No need to find new vulnerabilities
- No need to worry about timing, tracing, etc.
- Toolkits are readily available to allow the novice to perform DDoS
- Even distributed parts are very simple
2. Preys On Internet’s Strengths

- The Internet was designed to deliver lots of traffic
  - From lots of places, to lots of places
- DDoS attackers want to deliver lots of traffic from lots of places to one place
- Any individual packet can look proper to the Internet
- Without sophisticated analysis, even the entire flow can appear proper
Internet Resource Utilization

- Internet was not designed to monitor resource utilization
  - Most of it follows first come, first served model
- Many network services work the same way
- And many key underlying mechanisms do, too
- Thus, if a villain can get to the important resources first, he can often deny them to good users
3. Availability Of Attack Machines

- DDoS is feasible because attackers can enlist many machines
- Attackers can enlist many machines because many machines are readily vulnerable
- Not hard to find 1,000 crackable machines on the Internet
  - Particularly if you don’t care which 1,000
- Botnets numbering hundreds of thousands of hosts have been discovered
DDoS attacks don’t really harm the attacking machines

Many people don’t protect their machines even when the attacks can harm them

Why will they start protecting their machines just to help others?

Altruism has not yet proven to be a compelling argument for network security
4. Attacks Resemble Normal Traffic

- A DDoS attack can consist of vast number of requests for a web server’s home page.
- No need for attacker to use particular packets or packet contents.
- So neat filtering/signature tools may not help.
- Attacker can be arbitrarily sophisticated at mirroring legitimate traffic.
  - In principle
  - Not often done because dumb attacks work so well.
5. Lack Of Enforcement Tools

- DDoS attackers have never been caught by tracing or observing attack
- Only by old-fashioned detective work
  - Really, only when they’re dumb enough to boast about their success
- The Internet offers no help in tracing a single attack stream, much less multiple ones
- Even if you trace them, a clever attacker leaves no clues of his identity on those machines
What Is the Internet Lacking?

- No validation of IP source address
- No enforcement of amount of resources used
- No method of tracking attack flows
  - Or those controlling attack flows
- No method of assigning responsibility for bad packets or packet streams
- No mechanism or tools for determining who corrupted a machine
6. Poor Cooperation In the Internet

- It’s hard to get anyone to help you stop or trace or prevent an attack
- Even your ISP might not be too cooperative
- Anyone upstream of your ISP is less likely to be cooperative
  - ISPs more likely to cooperate with each other, though
- Even if cooperation occurs, it occurs at human timescales
  - The attack might be over by the time you figure out who to call
7. Effective Solutions Hard To Deploy

- The easiest place to deploy defensive systems is near your own machine
  - Defenses there might not work well (firewall example)
- There are effective solutions under research
  - But they require deployment near attackers or in the Internet core
  - Or, worse, in many places
- A working solution is useless without deployment
  - Hard to get anything deployed if deploying site gets no direct advantage