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