Prolog to Lecture 10
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

A Challenge to DDoS Defense

- Dropping traffic close to the target is too late
- Attackers increasingly overwhelming the target's ISP
- Ensuring poor service for the target
- So we need to defend the ISP
  - And maybe even further out

Why Is This a Problem?

1. The ISP and upstream network elements don’t know what to drop
2. They are in the business of delivering packets
   - Not dropping packets
3. They fear (business/legal) consequences of dropping the wrong things

What Would We Like?

- Targets should be able to inform ISPs of what to drop
- ISPs then implement those requests
- Traditional networking equipment makes this difficult
  - Especially in real time

SDN (Maybe) To the Rescue

- **S**oftware **D**efined **N**etworking
- Switches and routers that are more programmable
  - Flexibly and at high speeds
- Increasingly popular at ISPs
- Perhaps offering mechanism to deploy filters to combat DDoS

Some Challenges

- Do clients really know what they want dropped?
- Can they specify that in terms sensible for SDN equipment?
- Can we "push" filtering out far enough to be effective?
- Security issues
  - "DoS by SDN"