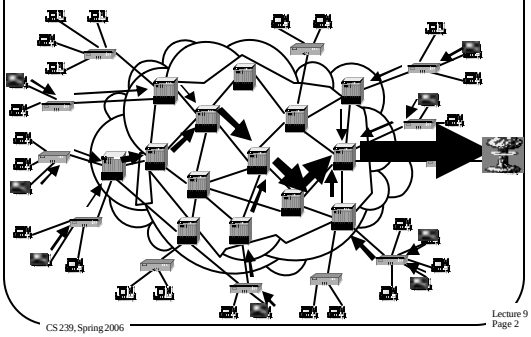
Distributed Denial of Service Attacks and Defenses
CS 239
Advanced Topics in Network Security
Peter Reiher
May 3, 2006

The Problem



Distributed Denial of Service (DDoS) Attacks

- Goal: Prevent a network site from doing its normal business
- Method: overwhelm the site with attack traffic
- Response: ?

Why Are These Attacks Made?

- Generally to annoy
- Sometimes for extortion
- If directed at infrastructure, might cripple parts of Internet
  - So who wants to do that . . .?

Attack Methods

- Pure flooding
  - Of network connection
  - Or of upstream network
- Overwhelm some other resource
  - SYN flood
  - CPU resources
  - Memory resources
  - Application level resource
- Direct or reflection

Why "Distributed"?

- Targets are often highly provisioned servers
- A single machine usually cannot overwhelm such a server
- So harness multiple machines to do so
- Also makes defenses harder

Yahoo Attack

- Occurred in February 2000
- Resulted in intermittent outages for nearly three hours
- Attacker caught and successfully prosecuted
- Other companies (eBay, CNN, Microsoft) attacked in the same way at around the same time

DDoS Attack on DNS Root Servers

- Concerted ping flood attack on all 13 of the DNS root servers in October 2002
- Successfully halted operations on 9 of them
- Lasted for 1 hour
  - Turned itself off, was not defeated
- Did not cause major impact on Internet
  - DNS uses caching aggressively

How to Defend?

- A vital characteristic:
  - Don't just stop a flood
  - ENSURE SERVICE TO LEGITIMATE CLIENTS!!!
- If you deliver a manageable amount of garbage, you haven't solved the problem

Complicating Factors

- High availability of compromised machines
  - At least tens of thousands of zombie machines out there
- Internet is designed to deliver traffic
  - Regardless of its value
- IP spoofing allows easy hiding
- Distributed nature makes legal approaches hard
- Attacker can choose all aspects of his attack packets
  - Can be a lot like good ones

Basic Defense Approaches

- Overprovisioning
- Dynamic increases in provisioning
- Hiding
- Tracking attackers
- Legal approaches
- Reducing volume of attack

Overprovisioning

- Be able to handle more traffic than attacker can generate
- Works pretty well for Microsoft and Google
- Not a suitable solution for Mom and Pop Internet stores

Dynamic Increases in Provisioning

- As attack volume increases, increase your resources
- Dynamically replicate servers
- Obtain more bandwidth
- Not always feasible
- Probably expensive
- Might be easy for attacker to outpace you

Hiding

- Don't let most people know where your server is
- If they can't find it, they can't overwhelm it
- Possible to direct your traffic through other sites first
  - Can they be overwhelmed . . .?
- Not feasible for sites that serve everyone

Tracking Attackers

- Almost trivial without IP spoofing
- With IP spoofing, more challenging
- Big issue:
  - Once you've found them, what do you do?
- Not clear tracking actually does much good
- Loads of fun for algorithmic designers, though

Legal Approaches

- Sic the FBI on them and throw them in jail
- Usually hard to do
- FBI might not be interested in "smal fry"
- Slow, at best
- Very hard in international situations
- Generally only feasible if extortion is involved
  - By following the money

Reducing the Volume of Traffic

- Addresses the core problem:
  - Too much traffic coming in, so get rid of some of it
- Vital to separate the sheep from the goats
- Unless you have good discrimination techniques, not much help
- Most DDoS defense proposals are variants of this

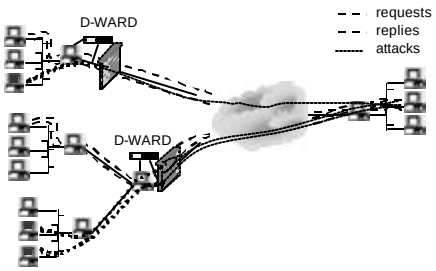
Approaches to Reducing the Volume

- Give preference to your "friends"
- Require "proof of work" from submitters
- Detect difference between good and bad traffic
  - Drop the bad
  - Easier said than done

D-WARD

- Source-end, inline defense system
- Compares observed flows with protocol-based models:
  - Mismatching flow statistics indicate attack
- Dynamic and selective rate-limit algorithm:
  - Fast decrease to relieve the victim
  - Fast increase when the attack stops and on false alarms
  - Detects, forwards legitimate connection packets
- Major questions:
  - Deployment incentives
  - Partial deployment issues

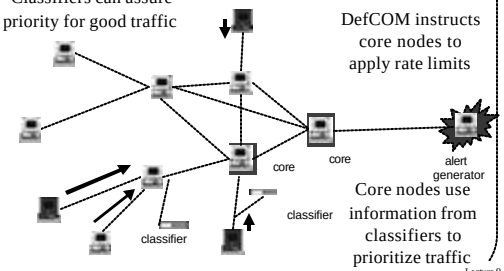
D-WARD in Action



DefCOM

Classifiers can assure priority for good traffic

DefCOM instructs core nodes to apply rate limits



Core nodes use information from classifiers to prioritize traffic