

Denial of Service Attacks

- Unlike other forms of computer attacks, goal isn't access or theft of information or services
- The goal is to stop the service from operating
 - To deny service to legitimate users
- This is usually a temporary effect that passes as soon as the attack stops

1

How Can a Service Be Denied?

- Lots of ways
 - Crash the machine
 - Or put it into an infinite loop
 - Crash routers on the path to the machine
 - Use up a key machine resource
 - Use up a key network resource
- Using up resources is the most common approach

2

Simple Denial of Service Attacks

- One machine tries to overload another machine
- There is a fundamental problem for the attacker:
 - The attack machine must be “more powerful” than the target machine
- The target machine might be a powerful server
- Can one typical client machine generate enough work to overcome a powerful server?

3

Denial of Service and Asymmetry

- Sometimes generating a request is cheaper than formulating a response
- If so, one attack machine can generate a lot of requests, and effectively multiply its power
- Not always possible to achieve this asymmetry

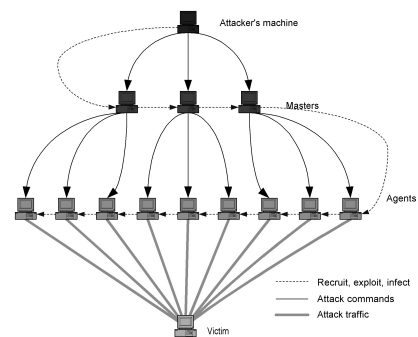
4

DDoS “Solves” That Problem

- Use multiple machines to generate the workload
- For any server of fixed power, enough attack machines working together can overload it
- Enlist lots of machines and coordinate their attack on a single machine

5

Typical Attack Modus Operandi



Is DDoS a Real Problem?

- Yes, attacks happen every day
 - One study reported ~4,000 per week¹
- On a wide variety of targets
- Tend to be highly successful
- There are few good existing mechanisms to stop them
- There have been successful attacks on major commercial sites

7

¹"Inferring Internet Denial of Service Activity," Moore, Voelker, and Savage, Usenix Security Symposium, 2002

Yahoo Attack

- Occurred in February 2000
- Resulted in intermittent outages for nearly three hours
- Estimated to have cost Yahoo \$500,000 due to fewer page hits during the attack
- Attacker caught and successfully prosecuted
 - But not due to cybertools
- Other companies (eBay, CNN) attacked in the same way at around the same time

8

Microsoft Attacks

- Target of multiple DDoS attacks
- Some successful, some not
- Successful one in January 2001
 - Attacked router in front of Microsoft's DNS servers
 - During attack, as few as 2% of web page requests were being fulfilled
 - As opposed to 97%, under normal load
- Solved by a better configuration of Microsoft's DNS servers

9

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
- Appears to have been the work of experts
- Did not cause major impact on Internet
 - DNS uses caching aggressively
 - Several root servers were provisioned enough
- Longer, stronger attacks might have succeeded
- The perpetrator of this attack is still unknown

10

Attacks on ClickBank and SpamCop

- Performed the weekend of June 21-23, 2003
- Floods of bogus HTTP requests
- Seemed to involve thousands of attack machines
- Prevented the companies from doing business
 - And filled up their log files quickly
- Defeated by installing sophisticated filtering
 - Though attacks continued after installation

11

Recent Attack on Port of Houston, TX

- A 19-year old generated DDoS attack on a female chatuser, Port of Houston was in the middle and got disabled
- Port's web service was not accessible to provide crucial data for ships' navigation

12

How Big Problem is DDoS Actually

- One study suggests around 4,000 attacks daily in the Internet
 - On all types of targets
 - Most short, but some quite long
 - Methodology used would not catch all attacks
 - Another study suggests it would miss 75% of all attacks
- Generally, no good data is available

13

How Big Problem is DDoS Potentially

- Much worse
- Little evidence that attacks to date are very serious
 - Mostly seem to be tests, hackers showing off, or based on limited political objectives
- Real attacks on serious targets are definitely possible
- What would be the effects?

14

Potential Effects of DDoS Attacks

- Most (if not all) sites could be rendered non-operational
- The Internet could be largely flooded with garbage traffic
- Essentially, the Internet could grind to a halt
 - In the face of a very large attack
- Almost any site could be put out of business
 - With a moderate sized attack

15

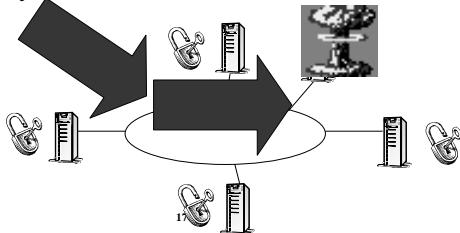
Who is Vulnerable?

- Everyone connected to the Internet can be attacked
- Everyone who uses Internet for crucial operations can suffer damages

16

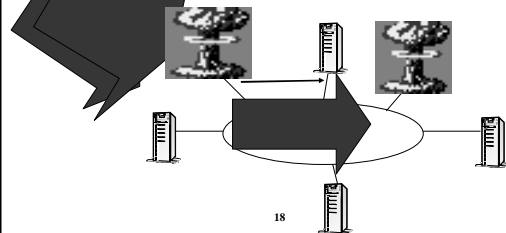
But My Machines Are Well Secured!

*Doesn't matter!
The problem isn't your vulnerability,
it's everyone elses'*



But I Have a Firewall!

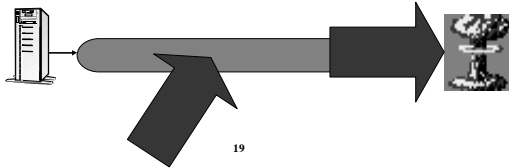
*Doesn't matter! Either the attacker slips his traffic into legitimate traffic
Or he attacks the firewall*



18

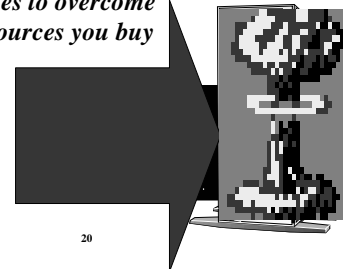
But I Use a VPN!

Doesn't matter!
The attacker can fill your tunnel with garbage
Sure, you'll detect it and discard it . . .
But you'll be so busy doing so that you'll have no time for your real work



But I'm Heavily Provisioned

Doesn't matter!
The attacker can probably get enough resources to overcome any level of resources you buy



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 again 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

So Why Isn't the Internet Dead?

- > If DDoS is so bad, why does the Internet (mostly) still work?
- > Most current and past attacks are small
 - > And unsophisticated
 - > Relatively weak defenses can protect against them
- > Few attackers seem very determined
 - > Mostly seem to be hackers "looking for a good time"

Will the Situation Ever Improve?

- > Maybe
- > Much research is going on
 - > Funded by government and industry
- > Vendors are building products
- > All parties recognize the dangers and the importance of the problem
- > But it's a really hard problem to solve
 - > Especially in the real world

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

25

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

26

2. DDoS 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

27

The Internet and Resource Utilization

- The Internet was not designed to monitor resource utilization
 - It's pretty much first come, first served
- 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

28

3. Easy 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 1000 crackable machines on the Internet
 - Particularly if you don't care which 1000
- Some reports suggest attack armies of tens of thousands of machines are at the ready

29

Can't We Fix These Vulnerabilities?

- Doubtful
- 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 for network security

30

4. Attack Can Look Like 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 currently done because dumb attacks work so well

31

5. Lack of Internet 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

32

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

33

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

34

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
 - Would your manager deploy something that only benefits other companies?

Attack Toolkits

- Widely available on the net
 - Easily downloaded along with source code
 - Easily deployed and used
- Automated code for:
 - Scanning – detection of vulnerable machines
 - Exploit – breaking into the machine
 - Infection – placing the attack code
- Rootkit
 - Hides the attack code
 - Restarts the attack code
 - Keeps open backdoors for attacker access
- DDoS attack code:
 - Trinoo, TFN(2K), Stacheldraht, Shaft, mstream, Trinity

DDoS Attack Code

- Attacker can customize:
 - Type of attack
 - UDP flood, ICMP flood, TCP SYN flood, Smurf attack
 - Web server request flood, authentication request flood, DNS flood
 - Victim IP address
 - Duration
 - Packet size
 - Source IP spoofing
 - Dynamics (constant rate or pulsing)
 - Communication between master and slaves

37

Implications of Attack Toolkits

- You don't need much knowledge or many skills to perpetrate DDoS
- Toolkits allow unsophisticated users to become DDoS perpetrators in little time
- DDoS is, unfortunately, a game anyone can play

38

DDoS Attack Trends

- Attackers follow defense approaches, adjust their code to bypass defenses
- Use of subnet spoofing defeats ingress filtering
- Use of encryption and decoy packets obscures master-slave communication
- Use of IRC channel for communication with slaves
- Encryption of attack packets defeats traffic analysis and signature detection
- Pulsing attacks

39

Implications for the Future

- If we solve simple attacks, DDoS perpetrators will move on to more complex attacks
- Possible future trends:
 - Larger networks of attack machines
 - Rolling attacks from large number of machines
 - Attacks at higher semantic levels
 - Attacks on different types of network entities
 - Attacks on DDoS defense mechanisms
- Need flexible defenses that evolve with attacks

40