Denial of Service

Unlike other forms of computer attacks, the 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
- Slowing down may be good enough
- This is usually a temporary effect that passes as soon as the attack stops

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
- Deny another service needed for this one (DNS)
- Using up resources is the most common approach

Floods
- Congestion control exploits
- Unexpected header values
- Invalid content
- Invalid fragments
- Large packets
- Impersonation attacks
One machine tries to bring down another machine. There is a fundamental problem for the attacker:

- The attack machine must be "more powerful" than the target machine to overload it OR
- Attacker uses approaches other than flooding
- The target machine might be a powerful server

Sometimes generating a request is cheaper than formulating a response e.g. sending a bogus packet is cheaper than decrypting this packet and checking that it’s bogus.

If so, one attack machine can generate a lot of requests, and effectively multiply its power.

Not always possible to achieve this asymmetry.

This is called amplification effect.

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.
Is DDoS a Real Problem?
- Yes, attacks happen every day
  - One study reported ~4,000 per week
- On a wide variety of targets
- Tend to be highly successful
- There are very few mechanisms that can stop certain attacks
- There have been successful attacks on major commercial sites

DDoS on Twitter
- August 2009, hours-long service outage
  - 44 million users affected
- At the same time Facebook, LiveJournal, YouTube and Blogger were under attack
  - Only some users experienced an outage
- Real target: a Georgian blogger

DDoS on Mastercard and Visa
- December 2010
- Parts of services went down briefly
- Attack launched by a group of vigilantes called Anonymous
  - Bots recruited through social engineering
  - Directed to download DDoS software and take instructions from a master
  - Motivation: Payback to services that cut their support of WikiLeaks after their founder was arrested on unrelated charges
  - Several other services affected

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

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

But My Machines Are Well Secured!
- Doesn’t matter!
  - The problem isn’t your vulnerability, it’s everyone else’s
Doesn’t matter! Either the attacker slips his traffic into legitimate traffic or he attacks the firewall.

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.

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

Wide 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
- Rootkits
  - Hide the attack code
  - Restart the attack code
  - Keep open backdoors for attacker access
- DDoS attack code

Attacker can customize:
- Type of attack:
  - UDP flood, ICMP flood, TCP SYN flood, Smurf attack (broadcast ping flood)
  - 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

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

Implications Of Attack Toolkits
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, IRC or P2P obscures master-slave communication
- Encryption of attack packets defeats traffic analysis and signature detection
- Pulsing attacks defeat slow defenses and traceback
- Flash-crowd attacks generate application traffic

Implications For the Future

- If we solve simple attacks, DDoS perpetrators will move on to more complex attacks
- Recently seen 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