Denial of service - Inability to get to some resource

- Blocks access to some resource based on something you have done
- This attack is highly used and powerful 300 gb/s in 2013 for attacks
- generate enough traffic to block network access
- If I am going to attack you I need more bandwidth then you.
- get a bigger pipe or DDOS distributed denial of service - get a lot of pipes
- Ping attack - icmp echo message (network interface responds and the stack doesn't deal with it) -attack just the network connectivity
- Defense is to turn pings off but you still get message so isn't entire defense
- TCP IP - born in a time of trust
- Source address spoofing - isp knows your IP address so it has the capability to do back trail checking
- Advertise fake addresses then trace back and analyse responses to see who was being attack
- TCP 3 way handshake - record a client wants a connection and will not remove from table until something occurs within the system. Attack is do a TCP send and server responds with an ack and waits for an ack. You just keep sending a connection request to the server but never send the ack. Get hit with 500,000 request then you start rejecting legitament packets.
- Amplification attack - DNS request attack - you send a little bit of data and get a ton back.
  
  UDP - connection-less protocol - send UDP packets to random ports on a machine. When you get one back then just start sending a ton of UDP packets

DOS categories that could be attacked: Network bandwidth, system resources, application resources