Denial of Service

- **In Feb. 2000, Yahoo's router kept crashing**
  - Engineers had problems with it before, but this was worse
  - Turned out they were being flooded with ICMP echo replies
  - Many DDoS attacks followed against high-profile sites
- **Basic Denial of Service attack**
  - Overload a server or network with too many packets
  - Maximize cost of each packet to server in CPU and memory
- **Distributed DoS (DDos) particularly effective:**
  - Penetrate many machines in semi-automatic fashion
  - Make hosts into "zombies" that will attack on command
  - Later start simultaneous widespread attacks on a victim

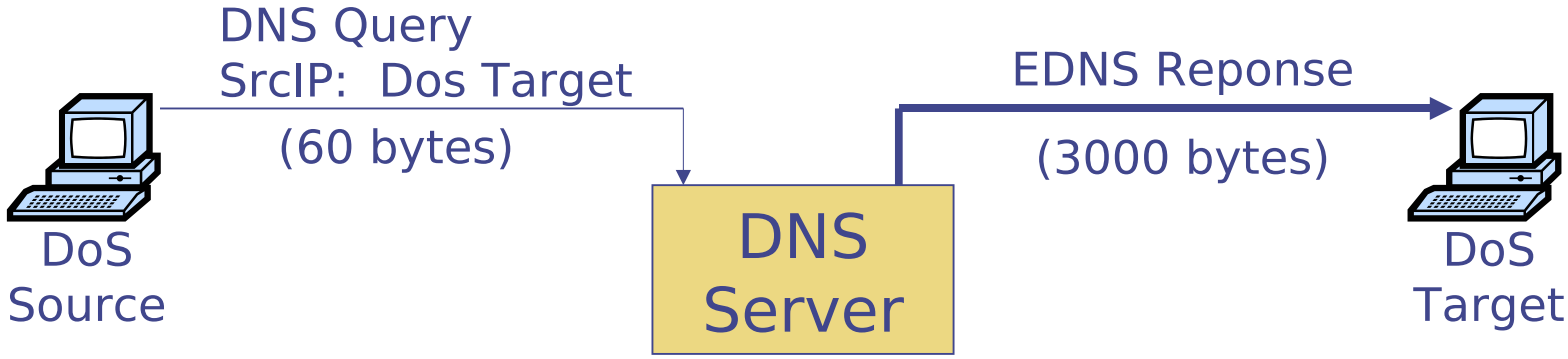
DoS attack overview

- **Class of attacks that just target availability**
- **Many motivations for Denial of Service (DoS)**
  - Extortion – E.g., pay us a small sum of money or we take down your off-shore on-line gambling site
  - Revenge – Spammers permanently shut down anti-spam company Blue Security
  - Bragging rights
- **Can DoS at many different layers**
  - Link, Network, Transport, Application, . . .

Warm up: simple DoS attacks

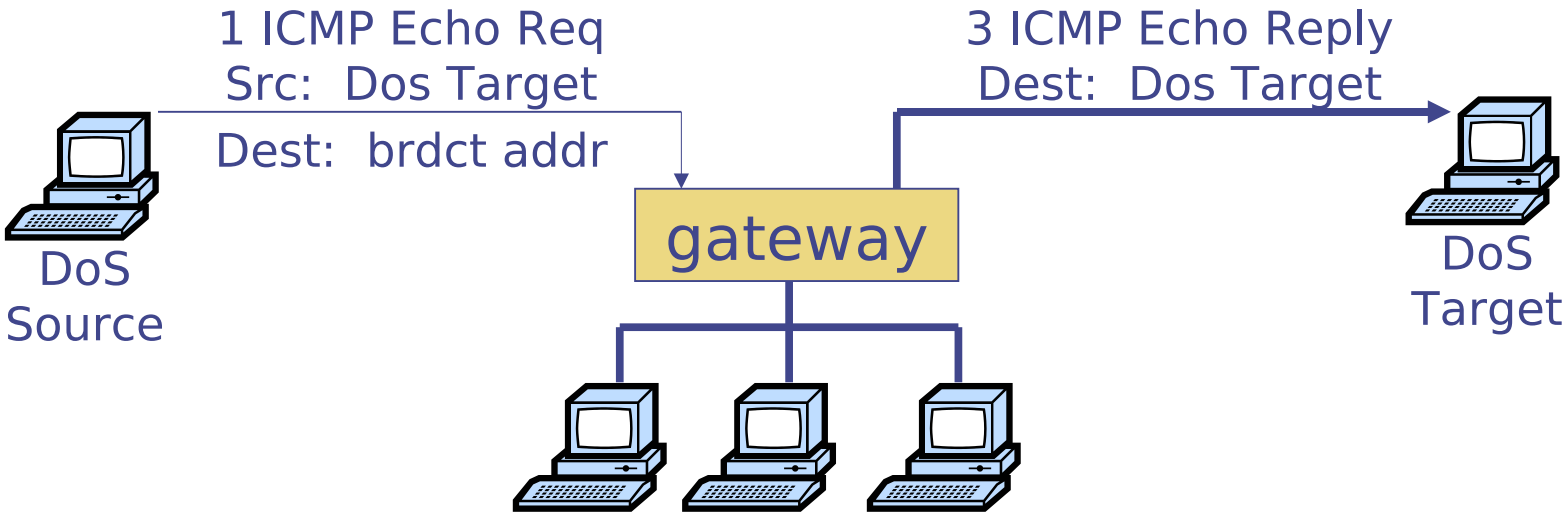
- **Jam a wireless network at physical layer**
  - Simple, maybe even with off-the-shelf cordless phone
- **Exploit NAV structure at 802.11 link layer**
  - NAV (Net Allocation Vector) used to suggest when network may be free (e.g., "after RTS/CTS exchange")
  - Use to reserve net repeatedly for max number of seconds
- **Flooding attack – e.g., flood ping**
  - `ping -f victim.com` – floods victim w. ICMP echo requests
- ***Amplification* can make attacks more powerful than resources directly available to attacker**

EDNS attack



- **Some EDNS [RFC 2671] responses $40\times$ size of query**
- **$\sim 500,000$ open DNS resolvers on Internet**
- **Flood victim w. DNS responses**
  - Send request forged to look like victim is source
  - Costs attacker only 60 bytes each
  - Go to many different DNS resolvers
  - All responses go back to same victim, 3,000 bytes each

SMURF attack



- **ICMP echo supports pinging IP broadcast address**
  - Useful to know what machines are on your network – all reply
- **Big amplification for flooding attack**
  - Compromise one machine on net
  - Ping broadcast address "from" victim IP
  - All machines will reply
- **Attack took down Yahoo!, buy.com, Amazon, in 2000**

The SYN-bomb attack

- **Recall the TCP handshake:**
  - $C \rightarrow S$: SYN, $S \rightarrow C$: SYN-ACK, $C \rightarrow S$: ACK
- **How to implement:**
  - Server inserts connection state in a table
  - Waits for 3rd packet (times out after a minute)
  - Compares each new ack packet to existing connections
- **OS can't handle arbitrary # partial connections**
- **Attack: Send SYN packets from bogus addresses**
  - SYN-ACKs will go off into the void
  - Server's tables fill up, stops accepting connections
  - A few hundred pkts/sec completely disables most servers

SYN-Bombs in the wild

- **MS Blaster worm**
  - Flooded port 80 of `windowsupdate.com` w. SYN packets
  - 50 SYN packets/sec (40 bytes each)
  - Randomized last two bytes of source IP address
- **Clients couldn't update to fix problem**
- **Microsoft's solution:**
  - Change the URL to `windowsupdate.microsoft.com`
  - Update old clients through Akamai

Other attacks

- **IP Fragment flooding**
  - Kernel must keep IP fragments around for partial packets
  - Flood it with bogus fragments, as with TCP SYN bomb
- **UDP echo port 7 replies to all packets**
  - Forge packet from port 7, two hosts echo each other
  - Has been fixed in most implementations

Application-level DoS

- **DNS supported by both TCP and UDP**
  - TCP protocol: 16-bit length, followed by message
  - Many implementations blocked reading message
  - Take out DNS server by writing length and just keeping TCP connection open
- **SSL requires public key decryption at server**
  - Can use up server's CPU time by opening many connections; relatively cheap to do for the client