Denial of Service

- **Denial of service** (DoS) an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.

Defining DoS not Easy

- four senders
- multi-hop paths
- timeout/retransmit
- B-D traffic at R2 dominates A-C traffic
DoS Threat Model

• Consumption of network connectivity and/or bandwidth
• Consumption of other resources. e.g. buffer, CPU
• Destruction or alteration of configuration information
  – Malformed packets confusing an application, causing it to freeze
• Physical destruction or alteration of network components

Targets of Attack

• End hosts
• Critical servers (disrupt C/S network)
  – Web, File, Authentication, Update
  – DNS
• Infrastructure
  – Routers within org
  – All routers in upstream path

Status

• DoS attacks increasing in frequency, severity and sophistication
  – 32% respondents detected DoS attacks [1999 CSI/FBI survey]
  – Yahoo, Amazon, eBay and Microsoft DDoS attacked
  – About 4,000 attacks per week in 2000
  – Internet’s root DNS servers attacked on
    • Oct. 22, 2002, 9 out of 13 disabled for about an hour
    • Feb. 6, 2007, one of the servers crashed, two reportedly "suffered badly", while others saw “heavy traffic”
  • An apparent attempt to disable the Internet itself
Two General Classes of Attacks

• Flooding Attacks
  – Point-to-point attacks: TCP/UDP/ICMP flooding, Smurf attacks
  – Distributed attacks: hierarchical structures

• Corruption Attacks
  – Application / service specific
    • E.g. polluting P2P systems

Classic Denial of Service Attacks

• Use simple flooding ping
  – From higher capacity link to lower
• Causing loss of traffic
  – Source of flood traffic easily identified
Source Address Spoofing

- Use forged (but routable) source addresses
  - Given sufficient privilege to "raw sockets"
  - Easy to create
- Generate large volumes of packets
  - Directed at target
  - With different, random, source addresses
- Cause same congestion
- Responses are scattered across Internet (back scatter)
- Real source is much harder to identify

Smurf DoS Attack

- Send ping request to broadcast address (ICMP Echo Req)
- Lots of responses:
  - Every host on target network generates a ping reply (ICMP Echo Reply) to victim
  - Ping reply stream can overload victim

TCP SYN Spoofing

- Another common attack
- Attacks ability of a server to respond to future connection requests
- Overflowing tables used to manage them
  - Hence an attack on system resource
TCP: Overview

- **point-to-point**: one sender, one receiver
- **reliable, in-order byte steam**: no "message boundaries"
- **pipelined**: TCP congestion and flow control set window size
- **send & receive buffers**

RFCs: 793, 1122, 1323, 2018, 2581

- **full duplex data**: bi-directional data flow in same connection
- **MSS**: maximum segment size
- **connection-oriented**: handshaking (exchange of control msgs) init’l sender, receiver state before data exchange
- **flow controlled**: sender will not overwhelm receiver

TCP segment structure

- **source port #**
- **dest port #**
- **sequence number**
- **acknowledgement number**
- **Receive window**
- **Urg data pointer**
- **Options (variable length)**
- **application data (variable length)**
- **Internet checksum (as in UDP)**

TCP Connection Management

**Three way handshake:**

**Step 1:** client host sends TCP SYN segment to server
- specifies initial seq #
- client address / port #, no data

**Step 2:** server host receives SYN, replies with SYNACK segment
- server allocates buffers
- specifies server initial seq. #

**Step 3:** client receives SYNACK, replies with ACK segment, which may contain data
• Attacker often uses either
  – Random source addresses
  – Or that of an overloaded server
  – To block return of (most) reset packets
• Has much lower traffic volume
  – Attacker can be on a much lower capacity link