Denial-of-Service Attacks

A survey of techniques and countermeasures.
CS 756

What is a DoS attack?

- An attack intended to impair or disrupt use of a service, resource, or utility.
- Look at utilities available to you, e.g., 911, electricity and water systems… what happens if 911 was flooded with?
- We look DoS attacks on the Internet’s users, organizations and infrastructures. Specifically, resource exhaustion attacks, a.k.a flooding attacks intended to overwhelm a system’s memory, CPU or network resources.
Email bombing attack

- Similar to SPAM only with the intention of exhausting your storage
- Countermeasure: filter, no complete solution!

TCP DoS attacks

- Recall TCP Three-Way Hand Shaking
- The victim will receive a segment with the SYN bit set to 1. The victim responds with the SYN-ACK and waits…
- The IP address of the source is forged, or the client never responds. The host keeps a TCP half-open connection.
- A dial-up PC can exhaust a host as the TCP connection queue is exhausted!
- Variant: SYN & source = destination = victim IP
- Even more variants: ACK and RST flags
TCP-SYN DoS attack defense

- No complete solution with current IP technology. Only methods to lessen severity of attacks
  - ISPs to update routers to filter packets
  - Hosts to update TCP-IP kernel
  - Increase size of connection queue
  - Decrease or introduce timeout period
- SYN cookies, now part of Linux

Distributed DoS (DDoS)

- Use more than one attacker via compromising other systems or constructing a network of attackers, or both
- Attacking tools include: TFN, TFN2k, trinoo, Stacheldraht, mstream and Trinity
- Sophisticated and well integrated networks
- Handler/agent or master/slave networks
- Stealth networks and mechanisms
DoS trends

- Internet infrastructure as target
- Shift to Windows users as zombies
- Reliance on social engineering
- Targeting routers
- Much faster exploitation of problems

Defense

- There is no complete solution
- Have a backup plan in case a DoS succeeds
- Keep your network updated
- Increase capacity if possible
- Establish good practices
- Anticipate attacks, be prepared to detect and react to them
Q&A