Network Denial of Service

John Mitchell

Course logistics

- Four more lectures
  - Today: Network denial of service
  - Tues: Firewalls, intrusion detection, traffic shapers
  - Thurs: Network security protocols
  - May 31: Paul Kocher, *Guest speaker*
- Project: due June 2
- Homework: due June 2
- Final exam: June 6

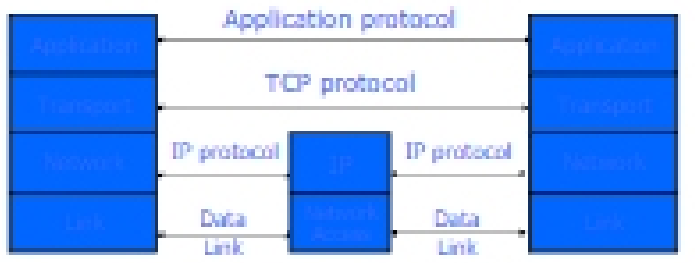
Outline

- Point-to-point network denial of service
  - Smurf, TCP syn flooding, TCP reset
  - Congestion control attack
- Distributed denial of service attacks
  - Coordinated attacks
  - Trin00, TFN, Stacheldraht, TFN2K
  - Bot networks
- Mitigation techniques
  - Firewall
  - IP traceback
    - Edge Sampling techniques
  - Overlay networks
    - Migration
    - Authentication

Sources

- Analysis of a Denial of Service Attack on TCP
  - Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, Diego Zamboni, Security & Privacy 1997
- Low Rate TCP Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)
  - Aleksandar Kuzmanovic and Edward W. Knightly, SIGCOMM 2003
- Practical Network Support for IP Traceback
  - Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson. SIGCOMM 2000
- Advanced and Authenticated Marking Schemes for IP Traceback
  - Dawn X. Song, Adrian Perrig. Proceedings IEEE Infocomm 2001
- MOVE: An End to End Solution To Network Denial of Service
  - A. Stavrou, A.D. Keromytis, J. Nieh, V.Misra, and D. Rubenstein

TCP Protocol Stack

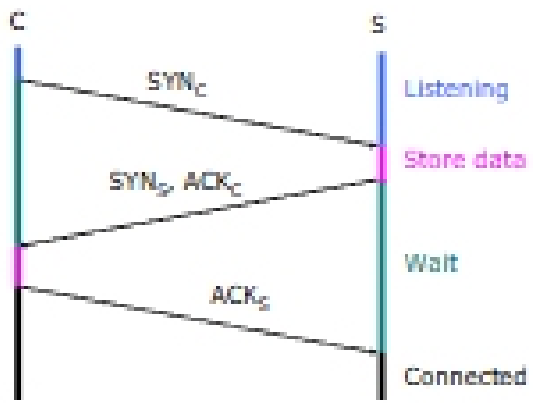


This lecture is about attacks on transport layer and below

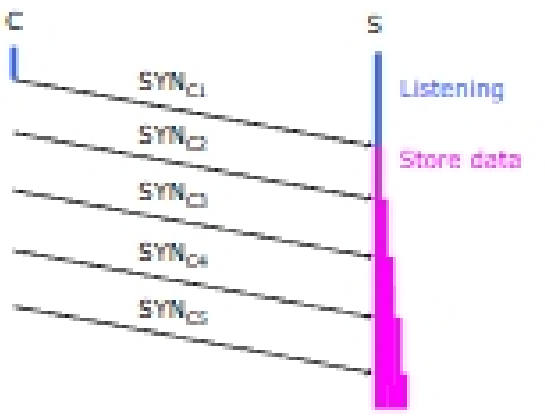
Point-to-point attacks

- Attacker chooses victim
- Sends network packets to isolate victim
- Goal of attacker
  - Small number of packets ⇒ big effect

TCP Handshake



SYN Flooding



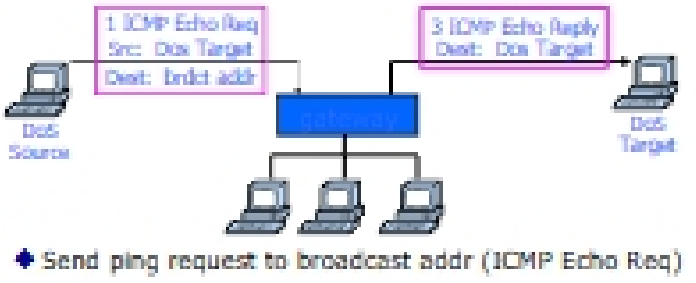
TCP Reset vulnerability [Watson'04]

- Attacker sends RST packet to reset connection
  - Need to guess seq. # for an existing connection
    - Naïvely, success prob. is $1/2^{32}$ for 32 bit seq. number
    - Most systems allow for a large window of acceptable seq. #'s ⇒ much higher success probability

Attack is most effective against long lived connections, e.g. BGP

Block with stateful packet filtering?

Smurf DoS Attack



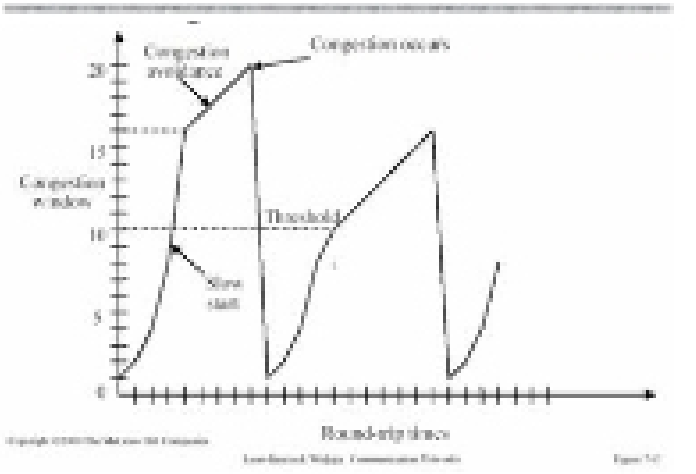
- Send ping request to broadcast addr (ICMP Echo Req)
- Lots of responses:
  - Every host on target network generates a ping reply (ICMP Echo Reply) to victim
  - Ping reply stream can overload victim

Prevention: reject external packets to broadcast address

TCP Congestion Control

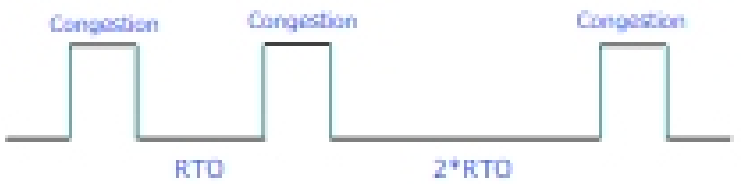
- Sender estimates available bandwidth
  - Starts slow and increases based on ACKS
  - Reduces rate if congestion is observed
- Two time scales
  - RTT is 10-100 ms ⇒ TCP performs AIMD
    - Additive Increase Multiplicative Decrease
    - Rises slowly, drops quickly (by half)
  - Severe congestion ⇒ Retransmission Timeout (RTO)
    - Send one packet and wait for period RTO
    - If further loss, RTO ← 2*RTO
    - If packet successfully received, TCP enters slow start
    - Minimum value for RTO is 1 sec

Pattern



Congestion control attack

- Generate TCP flow to force target to repeatedly enter retransmission timeout state



- Difficult to detect because packet rate is low
  - Degrade throughput significantly
  - Existing solutions only mitigate the attack

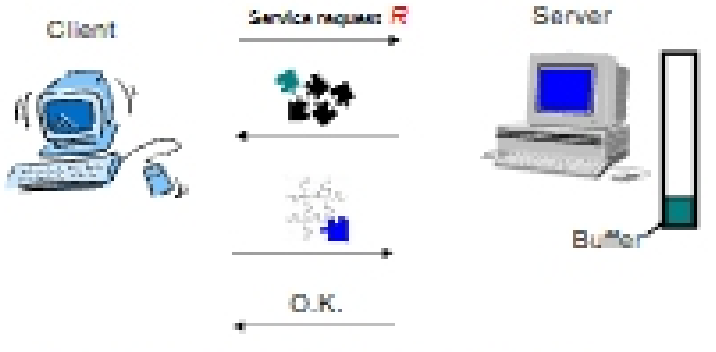
Defense against "connection depletion" attacks

Using puzzles to prevent DOS

- Basic idea
  - Sender must solve a puzzle before sending
  - Takes some effort to solve, but easy to confirm solution (e.g., hash collision)
- Example use (RSA client puzzle protocol)
  - Normally, server accepts any connection request
  - If attack suspected, server responds with puzzle
  - Allows connection only for clients that solve puzzle within some regular TCP timeout period

http://www.rsasecurity.com/rsalabs/node.asp?id=2050

The client puzzle protocol



http://www.rsasecurity.com/rsalabs/node.asp?id=2050

Outline

- Point-to-point network denial of service
  - Smurf, TCP syn flooding, TCP reset
  - Congestion control attack
- Distributed denial of service attacks
  - Coordinated attacks
  - Trin00, TFN, Stacheldraht, TFN2K
  - Bot networks
- Mitigation techniques
  - Firewall
  - IP traceback
    - Edge Sampling techniques
  - Overlay networks
    - Migration
    - Authentication

Distributed denial of service

- Attacker sets up network of machines
  - Break in by buffer overflow, etc.
- Attack machines bombard victim
- Attacker can be off line when attack occurs

Internet