Denial of Service (DoS) Attacks

Featured Speaker:

Gary Kessler

2/10/00

Featured Speaker: Gary Kessler

- Gary Kessler
  - Senior Network Security Analyst
  - Symquest Group
  - www.garykessler.net
  - kumquat@sover.net

2/10/00

Panel Members

Steve Taylor

Sharon Black

Steve Painter

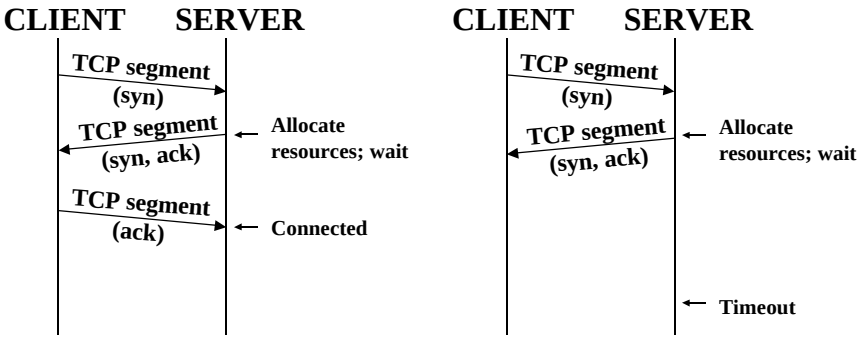
Denial of Service Attacks

- Becoming more common because they require limited technical skill and no access to the victim's server
  - SMURF attack
  - "PING Of Death"
  - TCP SYN DoS
- Can increasingly find detailed descriptions and attack tools on the Internet

Buffer Overflow Problems

- Buffer overflow exploits are legion on the Internet
  - E.g., sendmail, Windows 9x Telnet client, IE
- Many programming languages (e.g., C) do not automatically prevent array violations
  - And most programmers don't put in appropriate checks on input arguments
- Results range from crashing client applications to taking control of a server

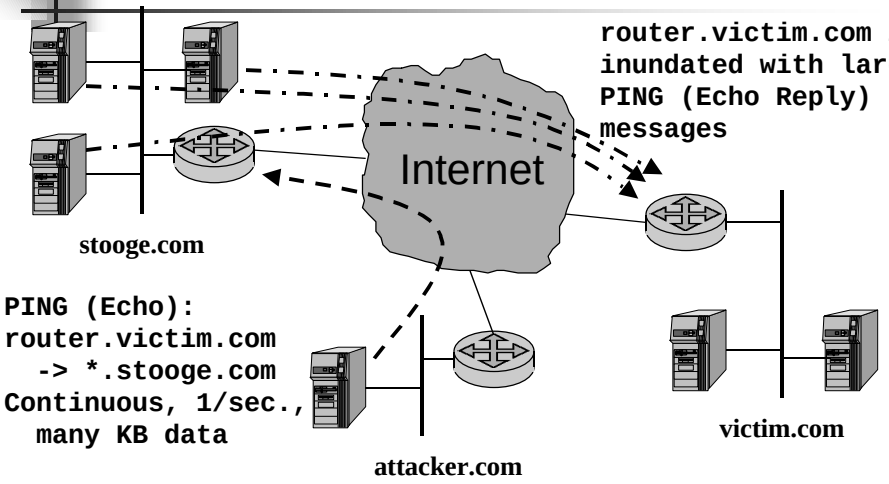
TCP SYN DoS Attack



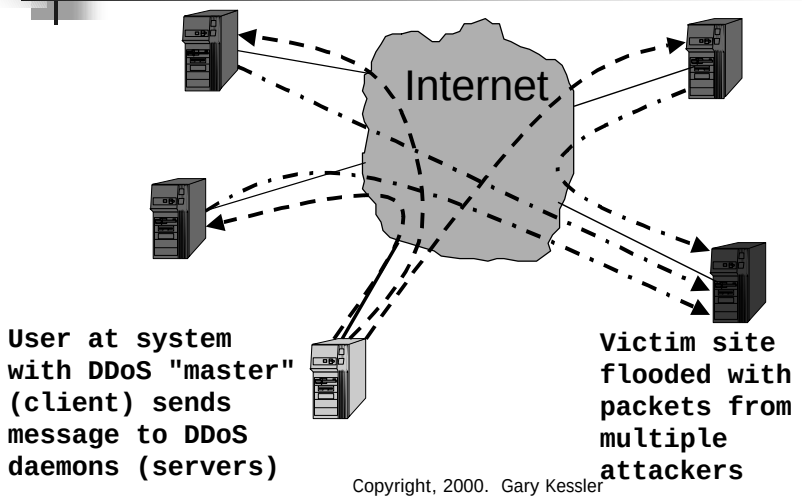
Normal TCP 3-way handshake

DoS: Server on hold waiting for client's response

SMURF DoS Attack



Distributed DoS Attacks



Distributed DoS Tools

- Trinoo (aka Trin00)
  - Launches UDP flood attack
  - Does not (yet) spoof source IP address
- Tribe Flood Network (TFN)
  - Launches UDP flood, TCP SYN flood, ICMP Echo Request flood, and SMURF attacks
- No good defense
  - Prevention requires cooperation