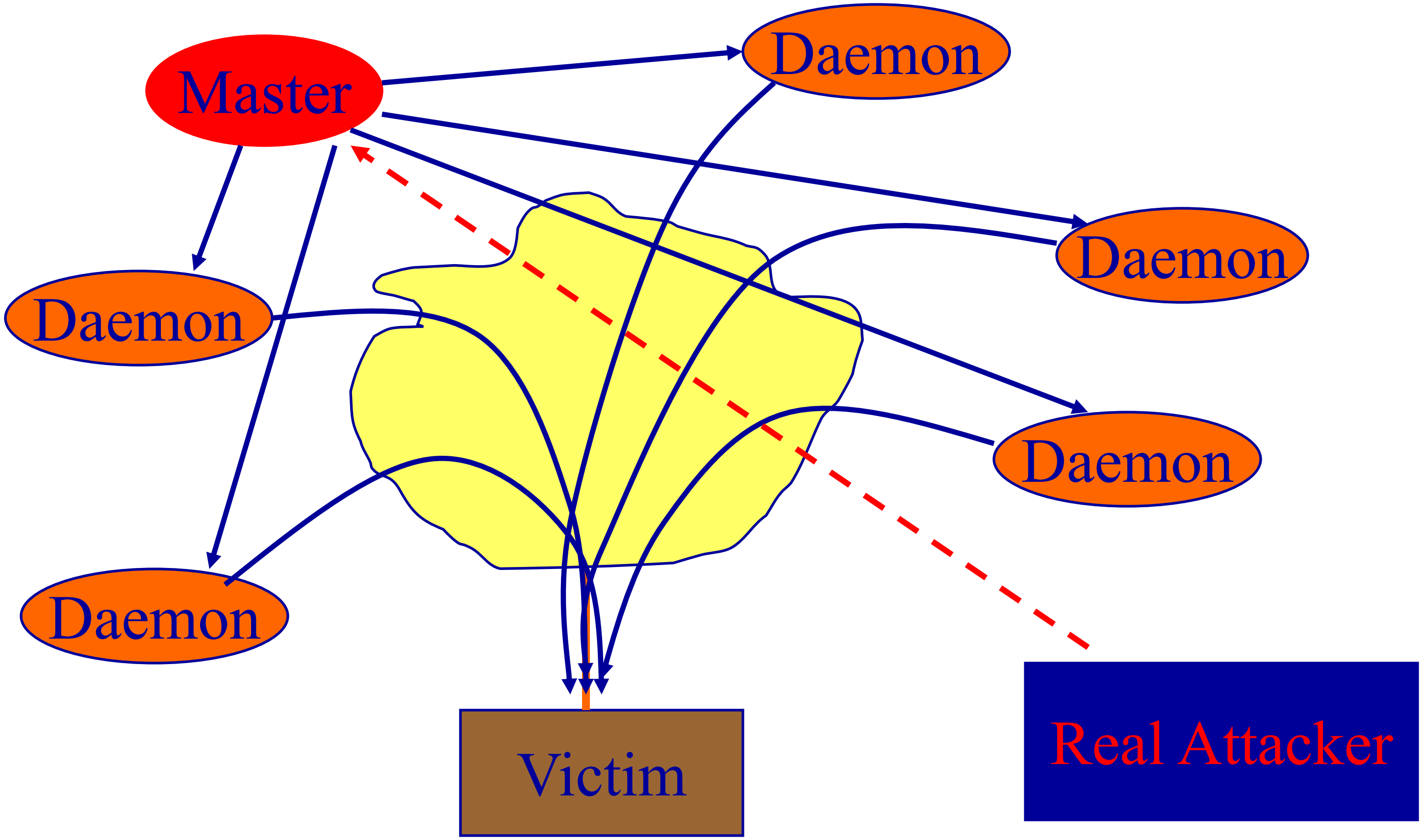
Distributed Denial of Service Attacks

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb

What Are DDoS Tools?

- Clog victim’s network.
- Use many sources (“daemons”) for attacking traffic.
- Use “master” machines to control the daemon attackers.
- At least 4 different versions in use: TFN, TFN2K, Trinoo, Stacheldraht.

How They Work



Agile Attackers

- Attack daemons implement many different types of DoS.
- “Smurf” – use directed broadcast to ask many remote machines to contact victim.
- “SYN Flood” – block access to given port number.
- UDP and ICMP flood – simply clog link.

Source-Address Spoofing

- Every Internet packet carries a return address.
- These tools use forged return addresses, partly to hide and (in one case) to trick other machines into attacking the victim.
- Attacks from legal source addresses are relatively easy to block.

How They Talk

- Trinoo: attacker uses TCP; masters and daemons use UDP; password authentication.
- TFN: attacker uses shell to invoke master; masters and daemons use ICMP ECHOREPLY.
- Stacheldraht: attacker uses encrypted TCP connection to master; masters and daemons use TCP and ICMP ECHO REPLY; rcp used for auto-update.

Deploying DDOS

- Attackers seem to use standard, well-known holes (i.e., rpc.ttdbserver, amd, rpc.cmsd, rpc.mountd, rpc.statd, etc.).
- They appear to have “auto-hack” tools – point, click, and invade.
  - Optional step: erase the log files; hide program.
- Lesson: practice good computer hygiene.

Detecting DDOS Tools

- Most current intrusion detection systems notice the current generation of tools.
- They work by looking for DDOS control messages.
- Naturally, these will change over time; in particular, more such messages will be properly encrypted. (A hacker PKI?)

What are the Strong Defenses?

- There aren’t any…

What Can ISPs Do?

- Deploy source address anti-spoof filters (*very important!*).
- Turn off directed broadcasts.
- Develop security relationships with neighbor ISPs.
- Set up mechanism for handling customer security complaints.
- Develop traffic volume monitoring techniques.

Traffic Volume Monitoring

- Look for too much traffic to a particular destination.
- Learn to look for traffic to that destination at your border routers (access routers, peers, exchange points, etc.).
- Can we automate the tools – too many queue drops on an access router will trigger source detection?

Can We Do Better Some Day?

- ICMP Traceback message.
- Enhance newer congestion control techniques, i.e., RED.

Warning – both of these are untested ideas. The second is a research topic.

ICMP Traceback

- For a very few packets (about 1 in 20,000), each router will send the destination a new ICMP message indicating the *previous* hop for that packet.
- Net traffic increase at endpoint is about .1% -- probably acceptable.
- Issues: authentication, loss of traceback packets, load on routers.

Enhanced Congestion Control

- Define an attack as “too many packets drops on a particular access line”.
- Send upstream node a message telling it to drop more packets for this destination.
- Traditional RED+penalty box works on flows; this works on destination alone.
- Issues: authentication, fairness, effect on legitimate traffic, implementability, etc.

References

- From CERT: CA-99-17, CA-2000-01, IN-99-07.
- http://www.cert.org/reports/dsit_workshop.pdf
- Dave Dittrich's analyses:
  - http://staff.washington.edu/dittrich/misc/trinoo.analysis
  - http://staff.washington.edu/dittrich/misc/tfn.analysis
  - http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
- Scanning tool:
  http://www.fbi.gov/nipc/trinoo.htm
- IDS vendors, ICSA, etc.