Fighting DDoS (3):
Types of Distributed DoS

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the previous article in this series, we looked at some fundamental types of denial-of-service (DoS) attacks. In this article, I introduce a few examples of techniques that attackers use to harness the power of multiple computers in slowing down or stopping a target system or network -- the distributed DoS or _DDoS_ attacks.

* * *

One of the earliest attack techniques that used the resources of multiple systems to overwhelm as target was the Smurf attack. In this DoS, the attacker used a dangerous feature of IP networks, the _broadcast address_. Sending a request (e.g., a ping) to the broadcast of a network reproduces the request and sends it to every IP address on that network. All of the systems receiving the ping can then respond to the request by returning the appropriate information to the originator of the ping. The DoS in the Smurf attack occurs when a system using forged IP headers sends a ping to a broadcast address on a very large network and fraudulently directs the responses to a third system, the victim. The victim can easily be flooded with spurious traffic that interferes with legitimate communications.

Some readers will be familiar with distributed processing using PCs on the Internet; in the collaboration called SETI@home <http://setiathome.ssl.berkeley.edu/>, which uses the power of over three million PCs and workstations owned by volunteers who download radio-telescope data and upload the results of analysis performed during quiet periods on their computers. The current crop of DDoS attacks use unprotected computers on the Internet as components of a large distributed-processing environment in much the same way as the legitimate distributed-computing projects.

DDoS tools today scan for vulnerable systems on the Internet and install "zombie" programs which then listen for specific encrypted messages from "master" programs controlled by the criminal hackers (often children) planning the DDoS attacks. At some point, the master sends out instructions on which IP address to attack using which DoS technique. Since the master can easily control hundreds or thousands of zombies, the resulting flood of spurious traffic directed at a target can easily overwhelm all resources and prevent access to the system under attack.

Some of the DDoS tools in use today are trin00, tfn (Tribe Flood Network), Stacheldraht, TFN2K, Shaft, and Trinity (and many others). See Dave Dittrich's resource page at <http://staff.washington.edu/dittrich/misc/ddos/> for an extensive list of documents discussing such tools.

* * *

In the next article in this series, I will look at some of the fundamental causes for the Internet's susceptibility to DDoS attacks.
M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.