

What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?

Lawrence R. Rogers

Software Engineering Institute Carnegie Mellon University Pittsburgh, PA

What is a Distributed Denial of Service (DDoS) attack?

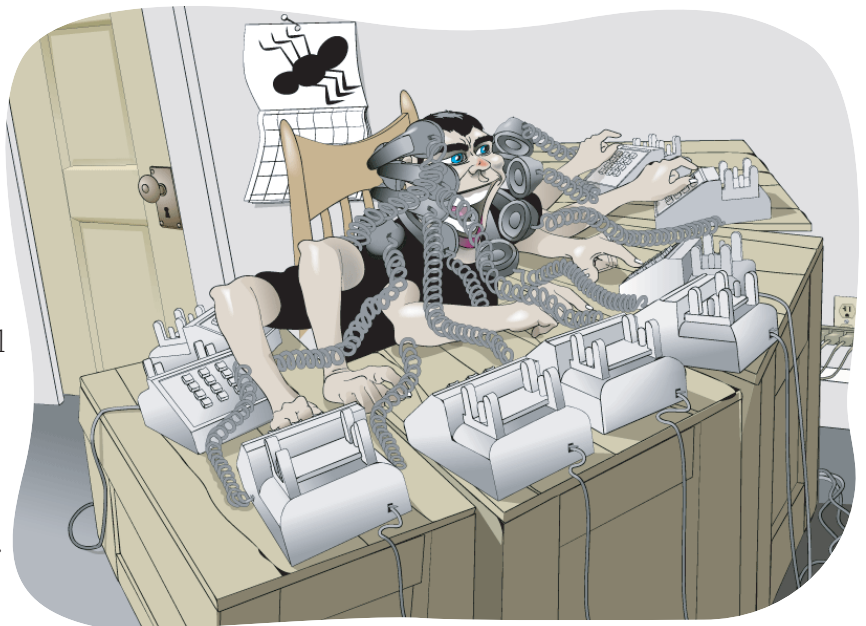
Have you ever tried to make a telephone call but couldn't because all the telephone circuits were busy? This may happen on a major holiday and often happens on Mother's Day. In fact, in the United States, telephone companies used to air commercials on television and radio that suggested you avoid peak calling times by making your calls early or late in the day.

The reason you couldn't get through is because the telephone system is designed to handle a limited number of calls at a time. That limit was determined by weighing the cost of having all calls get through all the time with the amount of traffic the system receives. If the total number of calls is always high, it makes economic sense for the telephone company to provide more capacity to match that demand. However, if the number of calls is low compared to the holiday peaks, then the telephone company will build networks that accommodate only the lower off-peak number of callers and advise their customers to avoid peak calling times. It's a basic matter of supply and demand.

Imagine that an intruder wanted to attack the telephone system and make the system unusable by telephone customers. How would they do this? One way would be to make call after call in an attempt to make all circuits busy. This type of attack is called a *denial of service*, or *DoS*, attack. In essence, the intruder has caused the telephone system to deny service to its customers. It is not likely that one caller working alone can tie up all telephone circuits.

To do that would require making as many calls as possible from as many telephones as possible. This is called a *distributed denial of service*, or *DDoS*, attack.

Computer systems can also suffer DoS and DDoS attacks. For example, sending an extraordinary amount of electronic mail to someone could fill the computer disk where mail resides. This means that people who use the computer with the full disk cannot receive any new email until the situation changes. While this is an older style of DoS attack, it is still popular today.



In addition, intruders have turned their efforts toward denying people the services provided by networked computers. Examples of frequently attacked services are the World Wide Webⁱ, file sharing services and, more recently, the Domain Name Service.ⁱⁱ Because so many of our computers are connected through the Internet, attacking one of these services can have a significant impact on the whole Internet community. For example, by launching a DoS attack on a popular merchant during a high sales period, the intruder affects not only that merchant, but everyone who is then unable to buy their products.

To deny these services to prospective users of a computer service, intruders run specially written computer programs that send extraordinary volumes of Internet “calls” to one of the computers that provides that service, similar to the way that an intruder can tie up the telephone system.

When a computer answers such a call, most often there’s no one on the other end, so answering the call turned out to be a waste of time. Unfortunately, the attacked service cannot tell this in advance, so it has to answer all calls placed to it. Answering each call takes time, and there’s only so much time available. It’s the supply and demand issue all over again.

In addition, the volume of traffic may be so high that the networks connecting the attacking computers to the victim’s computer may also suffer from lower performance. Just like the telephone system and service computers, these networks cannot handle traffic beyond a certain limit. Users wanting services from computers on those networks are denied those services, too. Those networks are also considered victims of a DDoS attack.

How do intruders wage a DDoS attack against a victim’s computer?

First, they build a network of computers that will be used to produce the volume of traffic needed to deny services to computer users. We’ll call this an *attack network*.

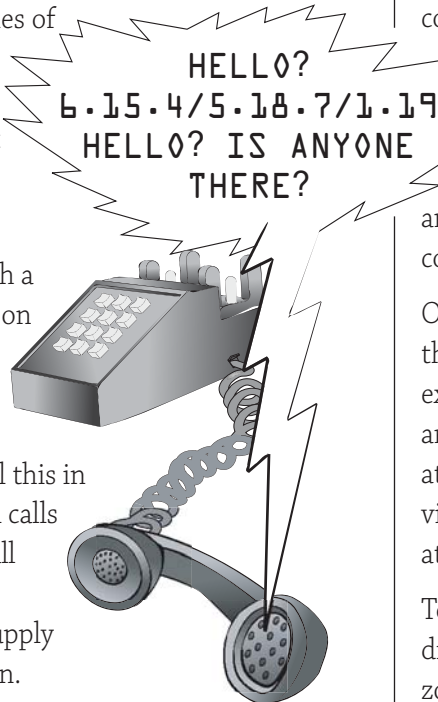
To build this attack network, intruders look for computers that are poorly secured, such as those that have not been properly patched, or those with out-of-date or non-existent anti-virus software. When the intruders find such computers, they install new programs on the computers that they can remotely control to carry out the attack.

Intruders used to hand-select the computers that made up the attack network. These days, however, the process of building an attack network has been automated through self-propagating programs. These programs automatically find vulnerable computers, attack them, and then install the necessary programs. The process begins again as those newly compromised computers look for still other vulnerable computers. Once a DDoS program has been installed on a computer, that program identifies the computer as a member of the attack network. Because of this self-propagation, large attack networks can be built very quickly. A by-product of the network-building phase is yet another DDoS attack, because searching for other vulnerable computers creates significant traffic as well.

Once an attack network is built, the intruder is ready to attack the chosen victim or victims. Some information security experts believe that many attack networks currently exist and are dormant, passively waiting for the command to launch an attack against a victim’s computers. Others believe that once a victim has been identified, the attack network is built and the attack launched soon afterward.

To reduce their chances of being discovered, intruders distribute their attack across computers in different time zones, different legal jurisdictions, and with different systems administrators. Intruders also make the electronic traffic they create appear to be from a computer different from the one that actually created it. This is called *IP spoofing*, and it is a commonly used method to disguise where an attack is really coming from. If the source of the attack is unknown, it is difficult to stop it, giving intruders free reign with a high likelihood of successfully remaining anonymous.

The MyDoom virus is an example of building such a DDoS attack network. In this case, the attack network was built not through technological vulnerabilities but rather through operational vulnerabilities. Computer system users were coaxed into executing a malicious program that was either sent as an email attachment or as a file downloaded through a Point-To-Point network connection, effectively enrolling their



computer system into the attack network. However, instead of remotely controlling the newly installed malicious program as previously described, the intruder designed it to automatically send significant amounts of traffic to www.sco.comⁱⁱⁱ on February 1, 2004 and www.microsoft.com on February 3, 2004. See <<http://www.us-cert.gov/cas/techalerts/TA04-028A.html>> for a detailed explanation of MyDoom. This alert also lists steps that can be taken to remove it from an infected computer system.

What can be done about DDoS attacks?

There are no short-term solutions to eliminate DDoS attacks. Today's best practices involve making computers and networks more resilient in the face of an attack. We call this *survivability*.

All systems have their limits. One way to make a system more survivable is to increase these limits; the more resources there are, the better the chances are that the system will survive an increased demand for use. To increase the telephone system's limits, the telephone company adds more circuits. For a web service, the webmaster might increase the number of connections that a web service can accept; for example, a site could add more web servers. This spreads the increased load over more computers and helps to ensure that no one computer operates too near its limit. The higher the limits of all the potentially affected systems – the network and the computers on that network – the better the chances that network will survive a DDoS attack.

You can do your part to ensure that your computers are never part of a DDoS attack network by following security best practices, such as those in *Home Computer Security* <<http://www.cert.org/homeusers/HomeComputerSecurity>>. Then, be alert to changes in your computer or network performance.

Ask yourself the following questions:

- Are your computers running noticeably slower than usual?
- Is your Internet connection slower than usual?
- Are the activity lights on your high-speed (cable or DSL) modem solid, or on almost all of the time?

Any of these could indicate that your computer system may be a participant in a DDoS attack network. If this happens to you, contact your Internet service provider (ISP) and follow their recommendations. Also, you should strongly consider turning off your computer system or your high speed modem. That will certainly stop the flow of DDoS traffic, though this is only a temporary solution.

If your computer system was a participant in a DDoS attack network, your system was compromised, and attack tools were installed on your computer. You'll need to determine what the intruders did and then repair the damage. The article *There IS an Intruder in My Computer – Now What ?* <<http://www.cert.org/homeusers/intruder2.html>> describes how to recover from an intrusion on your home computer.

Distributed denial of service attacks are a significant problem. These attacks will be with us for a while, though there is ongoing research on how to reduce them (see the *More reading* section below). Until then, DDoS is no (tele)phoney baloney!

More reading

You can find more reading for home users on the **CERT** web site <<http://www.cert.org/homeusers>>.

If you would like more technical details, you might be interested in reading the following:

- *Trends in Denial of Service Attack Technology* <http://www.cert.org/archive/pdf/DoS_trends.pdf>
- Papers on the topic of survivability <http://www.cert.org/nav/index_purple.html>
- *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* <<http://www.cert.org/archive/pdf/02sr009.pdf>>
See Part II on future directions to address the DDoS problem.
- i <http://www.computerworld.com/networkingtopics/networking/story/0,10801,60501,00.html>
- ii <http://www.computerworld.com/securitytopics/security/story/0,10801,75454,00.html>
- iii www.sco.com was changed to www.thescogroup.com in an attempt to defeat the MyDoom virus and is no longer a valid host name