

*Only a global response will protect against DDoS attacks, and a coordinated effort will require significant economic incentives to succeed.*

Xianjun Geng and  
Andrew B. Whinston



# Defeating Distributed Denial of Service Attacks

The notorious, crippling attack on e-commerce's top companies in February 2000 and the recurring evidence of active network scanning—a sign of attackers looking for network weaknesses all over the Internet—are harbingers of future Distributed Denial of Service (DDoS) attacks. They signify the continued dissemination of the evil daemon programs that are likely to lead to repeated DDoS attacks in the foreseeable future.

Simply put, a DDoS attack saturates a network. It simply overwhelms the target server with an immense volume of traffic that prevents normal users from accessing the server. In contrast to other types of DoS attacks that operate on an individual basis, these distributed attacks rely on recruiting a fleet of “zombie” computers that unwittingly join forces to flood the victim server.

Security experts generally acknowledge that the long-term solution to thwart future attempts of this type is to increase the security level of all

Internet computers. Attackers would then be unable to find zombie computers to control. Internet users would also have to set up globally coordinated filters to stop attacks early.

However, the critical challenge in these solutions lies in identifying the incentives for the Internet's tens of millions of independent companies and individ-

uals to cooperate on security and traffic control issues that do not appear to directly affect them.

We give a **brief introduction** to

- network weaknesses that DDoS attacks exploit,
- the technological futility of addressing the problem solely at the local level,
- potential global solutions, and
- why global solutions require an economic incentive framework.

## DDOS ATTACKS

Denial of service attacks are not a product of Y2K. In a cat-and-mouse game that has evolved as the victim's level of security has increased, DDoS attacks are merely state-of-the-art versions of previous strategies. Early DoS attacks damaged their target victims before being rendered harmless. In each case, the attacks capitalized on weak links in the network.

## Attacking network software bugs

Many types of networking software cannot cope with malformed Internet Protocol packets. When hit by such packets, the networking software crashes. Just one such example is the famous Teardrop attack, in which overlapped IP packets in a Transmission Control Protocol connection resulted in the crash of Windows NT. (For a reference to Teardrop, see <http://support.microsoft.com/support/kb/articles/Q179/1/29.ASP>.)

The patchwork solution to these attacks has been to fix the software bugs once identified.

## Inside

**Mixer's Economic Brilliance**  
**Common Misunderstandings about DDoS Attacks**

## Targeting network protocol problems

Another modus operandi of network attackers has been to focus on the weak link created by TCP's three-way handshaking requirement. In the *SYN flooding* method (see [http://www.cert.org/advisories/CA-96.21.tcp\\_syn\\_flooding.html](http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html) for details), the attacker initiates a connect request to the server but ignores the server's positive feedback, forcing it to waste valuable resources waiting for the connection acknowledgment. Too many pending connections eventually tie up all the server's resources, preventing legitimate users from accessing it. This attack does not saturate the server's processing ability or exploit its restricted network bandwidth; it merely overloads a bottleneck resource.

Two stopgap solutions have ensured that attacks of this type do not pose a fatal threat to e-commerce if these attacks originate from individual computers. First, new versions of network software optimize the protocol implementations to alleviate the bottleneck situation. Second, businesses can use a filter (which is always active) to block the attacking machine's IP once that machine initiates too many pending IP connections. This filter prevents repeated attacks. As effective solutions are available for companies to implement on their own, these two types of DoS attacks have not recently posed insurmountable problems to e-commerce.

## The DDoS attack: Attacking on all flanks

The critical innovation in the recent denial of service attack is its distributed nature. The DDoS attack strategy reveals the Internet's structural deficiency: Attackers can exploit its insecure and readily accessible channels to aggregate an enormous traffic volume that doesn't infiltrate but effectively jams the secure channels. John Elliott's "Distributed Denial of Service Attacks and the Zombie Ant Effect" (John Elliott, *IT Professional*, Mar./Apr. 2000, pp. 55-57) offers a concise explanation. The Computer Emergency Response Team (CERT) Web site ([http://www.cert.org/congressional\\_testimony/Fithen\\_testimony\\_Feb29.html](http://www.cert.org/congressional_testimony/Fithen_testimony_Feb29.html)) details the related technology.

An attack of this type is especially harmful to Web sites that place a high value on being open to the public, such as commercial sites and public service sites.

In brief, the DDoS attack strategy rests on the following four pillars:

- *Using the Internet's insecure channels.* A large proportion of computers on the Internet are not secure enough. They are easy prey for the zombie programs that disseminate like viruses on various platforms and take control. The CERT Web site offers solutions for various platforms.

## DDoS attacks use the Internet's insecure channels to gain access to victims.

- *Using huge traffic volume as the weapon.* Once enough zombie computers are under the attacker's control, the accumulated resources can bring down even sites like Yahoo that are designed for high traffic volume processing.
- *Completely circumventing the ultimate victim's security defense.* The DDoS attack does not infiltrate the victim computer. Rather, it blocks the access "roads," effectively making the computer's level of defense irrelevant.
- *Hiding the attacker's identity.* The DDoS attack's strategy of IP spoofing (using a faked source address in an IP packet) and attacking through a three-level hierarchical series of zombies makes the attacker's identity virtually impossible to trace.

A viable solution that can prevent DDoS attacks in the future must effectively address each of these strategic attack elements.

## PROPOSED SOLUTIONS

We classify proposed solutions to DDoS attacks into two broad categories: **local and global**. As the name suggests, local solutions can be implemented on the victim computer or its local network without an outsider's cooperation. Global solutions, by their very nature, require the cooperation of several Internet subnets, which typically cross company boundaries.

### Local solutions

Protection for individual computers falls into three areas. **Local filtering.** The timeworn short-term solution is to try to stop the infiltrating IP packets on the local router by installing a filter to detect them. The stumbling block to this solution is that if an attack jams the victim's local network with enough traffic, it also overwhelms the local router, overloading the filtering software and rendering it inoperable. According to Paul Holbrook, director of Internet technologies for CNN.com (one of the victims of the February DDoS attack), "... the problem was that the routers were so busy filtering that that in itself compromised us" (<http://www.cnn.com/2000/TECH/computing/02/09/denial.of.service/>).

**Changing IPs.** A Band-Aid solution to a DDoS attack is to change the victim computer's IP address, thereby invalidating the old address. This action still leaves the computer vulnerable because the attacker can launch the attack at the new IP address. This option is practical because the current type of DDoS attack is based on IP addresses.

System administrators must make a series of changes—to domain name service entries, routing table entries, and so on—to lead traffic to the new IP address. Once the IP change—which takes some time—is completed, all Internet routers will have been informed, and edge routers will drop the attacking packets.

## Mixer's Economic Brilliance

Here, we use Mixer, a hacker that created a popular DDoS tool, to represent the creators of all DDoS tools.

The success of a DDoS attack depends on how many zombie computers it captures. In principle, all Internet users should be active in defending their own computers from being seized as zombies. However, DDoS tool creators wish to reduce all Internet users' incentive to protect their computers, and surveys show that the creators have been very successful for the following reasons:

- All DDoS tools are very careful not to harm the zombie computers—they don't delete files or damage hardware. They only periodically send out huge traffic of pings, so they cause only minimal irritation to the zombie computer's owner.
- Once the DDoS tool initiates an attack, it generates traffic that has no financial cost to the zombie computer's owner under current fee structures.

Thus, the owner of a zombie computer has no firm incentive to defend against DDoS attacks. Once attacked, the victim e-commerce site finds that it is the only entity intensely affected. The attacker is happy to see its victim's helplessness because a lone defender in a DDoS attack can only lose.

Internet users and e-commerce organizations can do nothing about Mixer's friendliness toward zombie computer owners. But we can change traffic pricing to usage-based schemes, such as that of an e-postal system. Then, because of the huge traffic involved in a DDoS attack, a DDoS tool cannot avoid irritating many participants and consequently triggering a more organized resistance to such attacks.



requires the attacking computer to answer a random question before establishing the connection. The question should be easy for humans to answer but not computers—for example, “Which film won the Oscar for best picture in 2000?”

These and other client bottleneck solutions are based on the assumption that the attack is aimed at connection-based protocols such as TCP that support the Web. In February's attack, however, the zombie computers had no interest in communication; they just kept sending junk “ping” packets to the victim server. In other words, they were not interested in obtaining authorized access; they accomplished their goal by merely tying up the server and preventing others from accessing it. Given this goal, client bottlenecks will not deter a DDoS attacker.

### Global solutions

Clearly, as DDoS attacks target the deficiencies of the Internet as a whole, local solutions to the problem become futile. Global solutions are better from a technological standpoint. The real question is whether there is a global incentive to implement them.

**Improving the security of the entire Internet.** Improving the security of all computers linked to the Internet would prevent attackers from finding enough vulnerable computers to break into and plant daemon programs that would turn them into zombies. (For information on how to secure a computer or a local area network, see “Distributed Denial of Service Attacks and the Zombie Ant Effect,” John Elliott, Mar./Apr. 2000 *IT Professional*.)

**Using globally coordinated filters.** The strategy here is to prevent the accumulation of a critical mass of attacking packets in time. Once filters are installed throughout the Internet, a victim can send information that it has detected an attack, and the filters can stop attacking packets earlier along the attacking path, before they aggregate to lethal proportions. This method is effective even if the attacker has already seized enough zombie computers to pose a threat.

**Tracing the source IP address.** The goal of this approach is to trace the intruders' path back to the zombie computers and stop their attacks or, even better, to find the original attacker and take legal actions. If tracing is done promptly enough, it can help to abort the DDoS attack. Catching the attacker would deter repeat attacks.

Although this technique is now effective, attackers need only add a domain name service tracing function to the DDoS attack tools to render changing the IP address a futile process.

**Creating client bottlenecks.** The objective behind this approach is to create bottleneck processes on the zombie computers, limiting their attacking ability. Examples of this approach include

- *RSA Security Corp. Client Puzzles.* RSA's Client Puzzles algorithm (see <http://www.rsasecurity.com/rsalabs/staff/ajuels/papers/clientpuzzles.pdf>) requires the attacking computer to correctly solve a small puzzle before establishing a connection. Solving the puzzle consumes some computational power, limiting the attacker in the number of connection requests it can make at the same time.
- *Turing test.* Software implementing this approach

However, two attacker techniques hinder tracing:

- IP spoofing that uses forged source IP addresses, and
- the hierarchical attacking structure that detaches the control traffic from the attacking traffic, effectively hiding attackers even if the zombie computers are identified.

An effective solution would be to implement source IP address filtering, in which routers would refuse IP packets that did not come from valid sources. Implementing this would require Internet-wide consensus.

### GLOBAL SOLUTIONS: TECHNOLOGICAL VERSUS ECONOMIC FEASIBILITY

All three of the global solutions we've mentioned are technologically feasible. In fact, many organizations are taking action to implement all three: The importance of securing every computer and every organization has never before received so much publicity or enjoyed so many advocates. And the industry is attempting to implement coordinated filters through some form of union such as the Alliance for Internet Security (see <http://www.icsa.net>).

In recognition of a market need, anti-DDoS tools such as scanning detection software are also thriving and making the job of increased security easier and cheaper. For example, a simple free test available from Web Trends (<http://www.webtrends.net/tools/security/scan.asp>) can help find network holes in advance—before an attacker uses them.

However, fervent advocacy of global solutions does not necessarily result in actual implementation. Sample research by ICSA.net, for example, shows that less than 15 percent of all corporate users are filtering source IP addresses. An even smaller percentage of Internet service providers—less than 8 percent—are doing this type of filtering ([http://www.icsa.net/html/press\\_related/2000/3\\_23\\_00\\_NetLitmus.shtml](http://www.icsa.net/html/press_related/2000/3_23_00_NetLitmus.shtml)).

### Economic disincentive

Apparent economic disincentives result in a hesitation on the part of many to adopt the recommended global solutions. From the organization's and individual's perspectives, preventing a personal computer from being controlled by any potential attacker requires frequent—virtually constant—monitoring and updating, at considerable cost.

## Common Misunderstandings about DDoS Attacks

➤ **We have not successfully defeated DDoS attacks because we do not have effective technologies.**

**We do have effective technologies. Antivirus software is available to protect PCs from being captured as zombies. Coordinated filters can effectively stop the attacking traffic. Banning IP spoofing can help in easily and promptly identifying traffic sources.**

➤ **If we have the effective technologies, we will use them.**

**Not necessarily. If the cost of using the technology is higher than the benefit from using it, we will not use it. Most home computer owners do not see the need to employ costly real-time network monitoring and up-to-date antivirus software to protect their PCs. They especially see little need to protect against DDoS tools, which do not damage file systems.**

➤ **The Serbian Badman Trojan virus is not serious because it cannot self-replicate and self-mail.**

**The Serbian Badman Trojan virus conceals itself in movie files. Once executed, it turns the affected computer into a zombie. See <http://www.cnn.com/2000/TECH/computing/06/16/movie.virus.idg/index.html>.**

**Hackers do not want this virus to behave like the Melissa virus because then it may attract great public attention and be limited before any DDoS attack.**

➤ **There will be no major DDoS attacks in the future.**

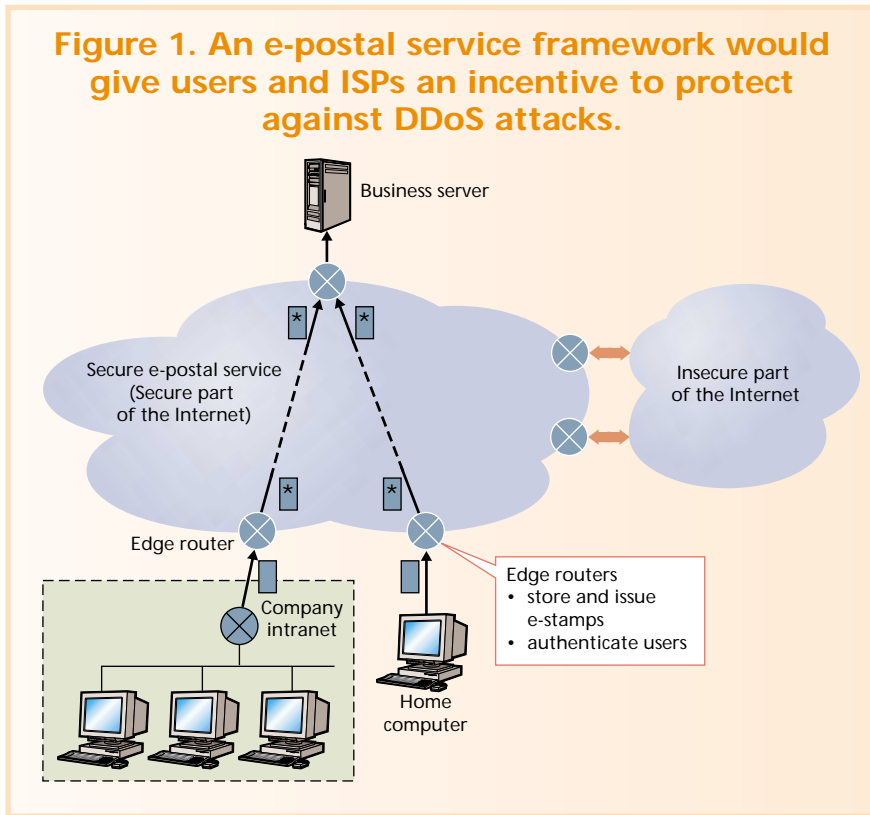
**Reports show that thousands of computers may have already been affected by the Serbian Badman Trojan virus and controlled by the virus sender. A coordinated attack from these thousands of computers may be capable of taking down any Web site.**



If the cost of protection is higher than the value of the data being protected, an economic disincentive clearly exists. This is particularly true as long as the only damage to the zombie computer is negligible—if all that is stolen is only some traffic. So in these days of flat monthly fee payments for Internet access, the owner of a zombie computer incurs no cost due to DDoS attacks, and the computer itself suffers no harm.

For ISPs, installing filters will reduce the overall transportation performance, as routers spend valuable computer cycles filtering. In addition, as long as the path of attack does not affect an ISP's business, what does it care about the attack? It still collects all those flat monthly fees.

**Figure 1. An e-postal service framework would give users and ISPs an incentive to protect against DDoS attacks.**



The paradox to this situation is that the converse is also true: The failure to cooperate harms social welfare—the benefits to businesses and consumers—from an economic perspective. According to the Yankee Group, a Boston consulting firm, the DDoS attack in February cost approximately \$1.2 billion.

**True potential cost**

We can expect higher costs for repeat attacks in the future, the ultimate price being a perception that e-commerce is structurally flawed. Such a perception could eventually thwart the huge economic potential of e-commerce and promise it offers to consumers in general. These costs are far higher than the cost of implementing coordinated filters, for example. From this perspective, implementing global solutions can indeed be determined economically efficient.

At the center of this paradox lies the flat monthly fee. This practice conveys to ISPs, corporations, and individuals the message that they are not responsible for control of their traffic. This encourages carelessness in traffic control, making the entire system vulnerable to DDoS attacks. The solution lies in creating the proper economic incentive structure for all parties.

**CONSTRUCTING ECONOMIC INCENTIVES**

A proper incentive structure would implement a sliding scale of usage-based fees, increasing the fee along with

traffic volume. The direct effect of a usage-based fee is an increase in the cost to zombie computers if they send out attacking traffic.

In particular, the cost could increase for high-performance, high-bandwidth computers that have the potential for sending huge traffic volume. These computers are most often located in corporations, governments, and universities, which represented the most dangerous zombie computers in February’s DDoS attacks. With a usage-based fee structure, the owners of such computers will have the greatest immediate incentive to take security actions.

The cost effect on modem users, on the other hand, may not be significant in the short term because of a modem’s limited bandwidth. However, the fast migration from modem to digital subscriber line and cable modem will gradually enable home PCs to play a major role in a DDoS attack. Under a usage-based fee structure, home

users would not initially have a large incentive to improve security, but that incentive would grow with their move to higher bandwidth Internet access.

As for ISPs, the incentive is immediately apparent: They would have to pay for every packet under this scenario, so a usage-based fee structure would give ISPs an urgent motivation to filter out all illegal packets.

The implementation of usage-based fees can be flexible. For example, with a careful analysis of consumer usage patterns and with strong traffic control tools, an ISP could still provide Internet access for a flat monthly fee if it is confident about traffic volume control, even if the ISP itself is paying usage-based fees to its network access supplier. This makes ISPs shoulder all the risks. However, this risk continuously increases as high-speed connections and bandwidth-consuming network tools become popular.

Introducing usage-based fees, the implementation of all three global solutions is consistent with the economic incentives of organizations, individuals, and ISPs.

Besides using usage-based fees, another option is to have all the routers involved in an attack owned by a single organization with an interest in protecting servers from being victimized. Under this scenario, a single player could initiate a global solution. Such an organization could arise from a union of ISPs or simply from a juggernaut ISP. The main drawback to this is that it encourages—in fact presupposes—the formation of a monopoly, which would have

an almost insurmountable competitive advantage over other ISPs. For this reason, we advocate the creation of a usage-based fee system.

### CONCEPT FOR AN E-POSTAL SYSTEM FRAMEWORK

The incentives inherent in a usage-based fee system suggest the need for what we call an *e-postal service framework* based on the introduction of a simple pricing mechanism, as shown in Figure 1. Such a framework focuses on constructing economic incentives so that people are willing to cooperate on traffic control, consequently benefiting social welfare.

Under this system, since users must pay a fee for all traffic, it is in the interest of each ISP to cooperate with adjacent ISPs to control traffic and reduce traffic costs. The entirety of cooperating ISPs constitutes an e-postal system that is secure enough to limit the possibility of being hacked. Because the e-postal system is a closed structure, ISPs need only implement security at the system's border. Core routers would transmit all packets within the e-postal system without further checks.

The all-important frontier of this e-postal system is controlled by edge routers, which monitor and control all the connected computers' traffic. To send out traffic, computers must buy e-stamps and store them on nearby edge routers. As an edge router allows an IP packet to enter the secure e-postal system, it charges the packet one e-stamp and attaches a stamp tag to the packet, indicating that it is valid.

Outside computer owners can set per-day or per-minute traffic limits, which edge routers can enforce to prevent abnormally large traffic volumes. Because such a system prohibits IP spoofing, tracing and stopping zombie computers is a relatively easy task.

Perhaps the major barrier to this framework is psychological. Internet users are accustomed to a fixed monthly subscription price or free access. Some effort will be required to persuade people to pay based on their surfing traffic. Governments can impose a per-packet tax as a feasible option.

**G**lobally coordinated solutions are indispensable for defeating the DDoS attack. Fostering such solutions will require proper economic incentives for all parties affected (directly or indirectly) by DDoS attacks. ■

*Xianjun Geng is a doctoral student in the Department of Management Science and Information Systems at the Graduate School of Business, University of Texas at Austin. He is also a research associate at the Center for Research in Electronic Commerce. Contact him at [gengxj@mail.utexas.edu](mailto:gengxj@mail.utexas.edu).*

*Andrew B. Whinston is the Hugh Cullen Chair Professor in information systems, computer science, and economics at the University of Texas at Austin. He is also the director for the Center for Research in Electronic Commerce. Contact him at [abw@uts.cc.utexas.edu](mailto:abw@uts.cc.utexas.edu); <http://crec.bus.utexas.edu>.*



COMING  
SOON

Distributed Systems Online