PIONEERING TECHNOLOGIES
FOR A BETTER INTERNET

Cs3, Inc.

5777 W. Century Blvd.
Suite 1185
Los Angeles, CA 90045-5600

Phone: 310-337-3013
Fax: 310-337-3012
E-mail: info@cs3-inc.com

MANAnet
Shield
A
Comprehensive Defense Against DDoS Attacks

(*Technical Summary Description*)

Deborah A. Taylor

Cs3, Inc
5777 W Century Blvd
Suite 1185
Los Angeles, CA 90045

Nature of Denial of Service (DoS) Attacks

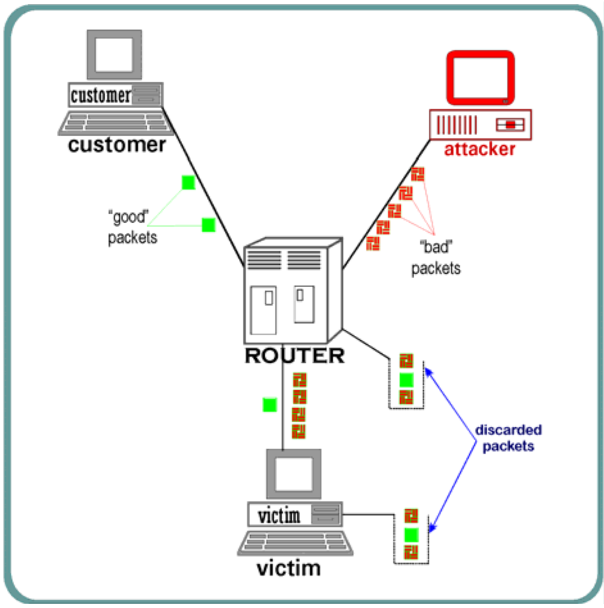
The goal of a DoS Attack on a server is to render the server unavailable to legitimate users. The best attacks are "*Distributed*" DoS or DDoS.

One common type of DDoS attack is packet flooding, where the victim's data communication bandwidth is filled with traffic from the attacker (or an army of "slaves" over which he has gained control), thereby preventing the communication the victim really wants. These attacks can be devastating.

Most organizations think of security as a characteristic of a particular site. This view may have merit for some problems, such as intrusion detection and virus protection, but a site cannot unilaterally defend itself against packet flooding DDoS attacks. In this case much of the damage is already done before the site can remedy the situation. In particular, the packets that the site wants to get from other places (such as its customers) do not arrive due to congestion in the network. This problem has to be fixed in the network that delivers packets to the victim.

A good percentage of attacks come from compromised computers within Universities and fast/permanent ISP connections to homes (*e.g., cable modem, DSL*).

Given the attack type, it then becomes difficult to trace the attacker(s) and hard to defend against the attack(s). Owners of the computers typically don't know their computers are being used like this. Unfortunately, there are many attack scripts available for DDoS attacks, which is clearly disproportionate to the number of proposed solutions.



Without a defense, the server will crash or slow down.

A good defense should not only keep the server running by suppressing the attack, it should let the real customers get through.

This is what Cs3's DDoS defense accomplishes…

Figure 1: DDoS Attack Illustration

Packet Flooding DDoS Attacks

Attacks cause loss of "good" (*i.e., customer*) traffic upstream from the victim because of congestion in the network.

This is the *key* technical problem in DDoS defense – and it is not easy to tackle.

The diagram illustrates how the flood from the attacker results not only in the victim being overwhelmed by "bad" traffic, but the fact that customers' "good" traffic could get discarded upstream from the victim.

The primary objective of the Cs3 defense is to thwart packet flooding attacks, where an attacker tries to disrupt data communication intended for the victim by using up all of his bandwidth.

A secondary objective is to defend against a related class of attacks where the attacker tries to use up some other resource, such as http (web) service.

Implications for DDoS Defense

The fact that customers' traffic maybe getting lost further upstream, has profound implications for DDoS Defense. In fact, it makes it fundamentally different from other kinds of security problems!

Guiding Principles for Cs3 Defense

There are basic assumptions and principles that have given rise to the Cs3 DDoS Defense. These principles essentially emerge from understanding the nature of the DDoS problem and the architecture of the present-day Internet.

Infrastructure Cooperation & Changes Needed:

The assumption is that most of the infrastructure is *not* controlled by the attacker. The Cs3 DDoS principles are predicated upon the following tenets:

1. It's virtually impossible to tell "good" from "bad" packets.
2. Protocols should provide foundation for defense to the extent possible, making the infrastructure less vulnerable to DDoS attacks.
3. Expect more cooperation from nearby routers.
4. A defense solution should not use data controlled by the attacker.
5. Smooth the transition from the present to the desired state as much as possible.
6. Avoid pitfalls of virus scanning model – which tries, in vain, to keep up with attackers' methods.
7. Best to eliminate attacks close to the attacker.
8. Ensure that any defense is not "for the greater good" because ISPs have simply not done even what is minimal *(e.g., ingress filtering of bad source addresses)*.

Armed with these principles, Cs3 has developed solutions to aggressively mount a defense against both *incoming* and *outgoing* DDoS attacks.

Defending Against Incoming Attacks

Defense against incoming attacks involves cooperation between routers and sites.

By modifying routers to not forward floods quite so eagerly Cs3 essentially makes the infrastructure DDoS resistant. A modified router will slow down traffic from specific places under the request of its neighbors.

Each site is responsible for knowing when it is being attacked (done by a modified firewall).

When attacked, each modified firewall contacts its neighbors to filter or slow the attack traffic. A neighborhood of cooperating routers around a site offers excellent DDoS protection by making the site harder to attack from outside the neighborhood.

Modified Router Details

Cs3 Router marks packets with path information – very much like a post office marking the letters that go through it. This is an enhancement of the Internet Protocol (IP), and as such is referred to as **Path Enhanced IP**, or **PEIP**. Usage of PEIP creates independent and reliable path data that is not controlled by the attacker.

In addition to PEIP, the router implements **Places-based Fair Queuing** (**PLFQ**); and is therefore able to:

- Schedule forwarding service equitably using path data – called "**Fair Service**";
- Effectively slow a flood from some place so that it cannot dominate;
- Make the Internet inherently DDoS resistant through fair service;
- Provide rate limiting/ filtering service to its nearest neighbors. When requested, the router will filter or rate limit traffic from specific paths.

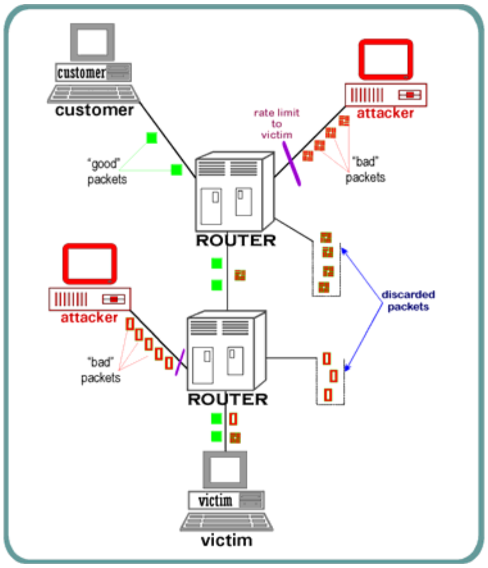


Figure 2: PEIP & PLFQ Example

Figure 2 shows how fair service works to protect the victim from DDoS attacks. The router 2 hops away from the victim serves the customer's traffic in preference to the flood from the attacker in order to be fair to the customer's relatively small bandwidth requirement. PEIP enables the router to distinguish customer traffic from attack traffic. Note that the defense not only slows the packets from the attacker, but, most importantly, lets the customer's packets through to the potential victim.

You might notice that fair service actually allows some proportion of the attacker's traffic through as well. This might still be too much for the victim in some cases. With the help of the Firewall component of the DDoS defense, we can do better than fair service.

Modified Firewall Details

Firewalls address the concerns (and, indeed, the important roles) of individual sites in the DDoS defense scheme. Cs3's Firewall has several important extensions to traditional firewalls:

- The Cs3 Firewall implements PEIP and PLFQ, exactly as described for a router. This enables this device to understand the path information in the packets it receives.
- The Firewall features rate limits for "unexpected packets" – those packets that are not replies to earlier packets in the opposite direction. Most DDoS attacks rely on the fact that they can send requests without ever looking for or processing the replies to those requests. Established 2-way (TCP) conversations are served as fast as fair service will allow, but requests to establish such connections need not be. This relatively simple strategy throttles most known DDoS attacks.
- The Firewall is where you can really detect that you are under attack. At the Firewall, thresholds can be set to reflect site-specific attack parameters.
- When an attack is detected, the Firewall contacts its upstream, cooperating neighbor (i.e., router) to slow down or filter traffic with specific path.

The modified Firewall plays a crucial role in improving the Fair Service defense, as is analyzed next.

How DDoS Defense Works

Fair Service neighborhoods guarantee that only a small portion of the attack traffic reaches the victim and that most of the customer's traffic will reach the victim -- customers get their "fair share" (as shown in Figure 2).

With the Firewall component:

- Slowing of unexpected packets ensures attacks are further throttled at the edge of the victim's network;
- DDoS defense improves because once an attack is detected, the Firewall can eliminate the attacker's fair share by requesting that the cooperating router (namely its upstream neighbor) slow down traffic with that path severely.

Effectiveness of Defense

The most impregnable DDoS defense starts with cooperative neighborhoods of "fair service" routers protecting each site.

Larger neighborhoods afford better defense because the number of places is larger. Note that there is no need for universal compliance to get the benefit – simply getting immediate neighbors (i.e., your ISPs) can help a great deal.

Each neighborhood is free to use its own PEIP scheme. One large neighborhood like that of a single large ISP or Government installation can produce immediate benefits. If the neighborhood is too large, trust in routers farthest away may or can dissipate.

Limits of Cs3 Incoming Defense

Communication within points inside the neighborhood is always protected. However, an attacker '**A**' outside the neighborhood can attack communication between a place '**I**' inside the neighborhood and another place '**O**' outside the neighborhood if either:

- ***A*** can flood a link outside the neighborhood (where the Cs3 defense has no control) along the path between ***O*** and ***I*** ; -or-
- ***A*** can send along the link by which traffic from ***O*** to ***I*** enters the neighborhood.

In this case the neighborhood cannot distinguish between traffic sent by ***O*** and by ***A***, so when ***A*** sends enough (if that is possible) then traffic from ***O*** might be dropped. This requires ***A*** to control a machine "in the right place". That's more likely if ***A*** controls more machines, less likely if ***I*** is inside a larger neighborhood.

Fair Service is not adequate, if the attacker simply abuses some service. [For example, repeated file downloads is not a flood. But it is an attempt to deny service.] **Historical Places-based Queuing** (**HPLFQ**) that is an extension to PLFQ, will resolve this type of attack. It will track usage over a period of time, and provide fair service for new requests using data over that interval.

There is a huge problem if a "fair service" router is compromised without the Cs3 defense in place. With the defense, there is still a problem, but it will depend on where the compromised router is relative to you. If it is your closest neighbor, then it will affect all communication through that router – meaning whatever "fair service" allocates to that router would be compromised badly. However, other communication through non-compromised routers will be fine.

While large neighborhoods help the DDoS defense, it may not be a good idea to trust the path data beyond a distance. At configuration time, the devices must be told which places are to be included in fair service allocation, and how much service each is to be allocated if there is contention. Not all neighbors are treated equally by Cs3 devices – you can choose to place more trust in some neighbors than others.

Path data (like packet sources) can be spoofed, which in turn reduces this problem to that of a compromised router above. The solution is to not trust all path information equally.

The Cs3 approach does not present impossible or difficult infrastructure changes. One can modify infrastructure (swapping out traditional routers and firewalls for Cs3 devices) gradually and incrementally.

Even small neighborhoods offer DDoS protection, and each new neighbor becoming PEIP-compliant assists in improving the quality of the defense incrementally.

Outgoing Attacks: The Reverse Firewall ®

The capabilities of the Firewall described earlier are actually symmetric. Firewalls can defend against OUTGOING attacks, because the basic notions of PEIP and PLFQ apply to outgoing packets too! Rate limiting of outgoing unexpected packets also reduces flood attacks to a trickle.

A Reverse Firewall is more effective for outgoing attacks because the "inside" network topology is simpler than that of the Internet. In short, we do not need cooperative routers with PEIP to tell us where traffic is truly coming from. One can detect where the attack is coming from down to the smallest subnet possible.

With some infrastructures (*e.g., cable modems or other network constructs wherein packet sources can be accurately identified*) Reverse Firewall performance is even greater because identification of the actual host that is originating bad traffic can be done.

The Reverse Firewall®

The Reverse Firewall provides direct value to the ISP, University or Enterprise that acquires the device because it protects the valuable internal communication between the users of the infrastructure during an attack – even if the attack comes from the outside!

Reverse Firewall Benefits are:

- Protection of the outside from attacks that originate inside the network;
- Protection of the desirable communications of legitimate customers of the infrastructure during attacks –whether the attacks come from the inside or outside.
- Protection of the owner of the infrastructure from liability and embarrassment caused by attacks; and
- Detection of the bad traffic source and notification to designated network administrators to take additional security steps to address the underlying security problem.

Reverse Firewall does not replace virus scanning or Intrusion Detection Systems (IDS) and other security procedures because it does not prevent "zombification" or infestation of machines:

Virus scanning and IDS solve more general computer security problems outside the DDoS context. Reverse Fire-Wall is a valuable additive in the defense arsenal for two reasons:

- Reverse Firewall makes known when the infrastructure may need attention and restricts the spread of the infestation and attacks greatly; and
- Gives you time to act to take care of your infrastructure while retaining availability of the network communications as much as feasible.

For example, Reverse Firewall would not have stopped Code Red or NIMDA infestations on individual computers, but it would have slowed their spread to a crawl and provided network administrators time to react. These, and most worms in their family, spread through rapid port scanning – which is an example of an unexpected packet. The Reverse Firewall severely limits the rate of such packets, making it harder for DoS attacks to be mounted.

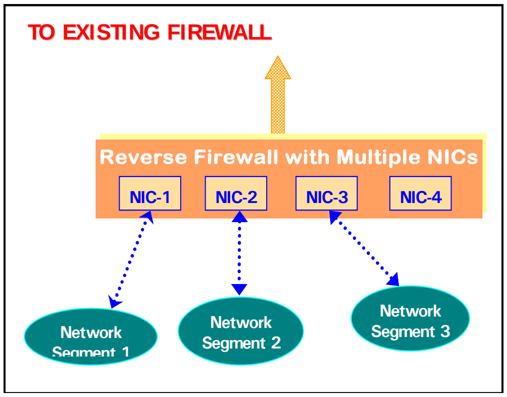


Figure 3: Fair Service to Each Network Segment

Reverse Firewall Deployment

Reverse Firewall has multiple NICs that can be used to distinguish traffic from different internal subnets. A single Reverse Firewall can guard up to five internal networks. Communication between non-attacking segments is essentially protected even during attacks from the inside or outside.

In some infrastructures, such as cable modem or other network configuration regimes, the Reverse Firewall can do even better by using packet source information available in each network segment (*e.g., MAC address of the cable modem*). It is most critical that the attacker cannot forge such information.

The only difference between the Reverse Firewall and the modified firewall for incoming DDoS defense is the ability to contact upstream routers. This is not a necessary capability for Reverse Firewalls because it focuses on outgoing traffic.

Once PEIP gains more acceptance, and cooperative neighborhoods of fair service routers become available, the Reverse Firewall can quite easily be extended to play the role of the firewall in the comprehensive defense against incoming DDoS attacks.

DDoS Defense Product Summary

To summarize, the Cs3 DDoS defense consists of devices that can be deployed to combat both incoming/outgoing flood attacks, including the related DDoS attacks like Reflection Packet Floods, “Over-Usage” attacks and SYN floods.

An important result of using the devices is an Internet that is inherently DDoS resistant. That is the best way to discourage attacks.

The Cs3 DDoS defense is intended to automate the current manual solution of calling the ISP to filter or throttle traffic. This might work for really large customers whose size might induce a level of extraordinary responsiveness on the part of the ISP. It is certainly not a suitable solution for smaller customers.

White Papers written about MANAnet technology and DDoS attacks that provide detailed narratives on methodology and solution propositions:

1. Cs3, Inc.; *Towards A More Secure and Robust Internet;* http://www.cs3-inc.com/pubs/internet-security-issues.pdf
2. D. Cohen and K. Narayanaswamy; *Changing IP to Eliminate Source Forgery;* http://www.cs3-inc.com/pubs/eliminating-source-forgery.pdf
3. D. Cohen, K. Narayanaswamy and Fred Cohen; *A Fair Service Approach to Defending Against Packet Flooding Attacks;* http://www.cs3-inc.com/pubs/fair-service-ddos-defense.pdf
4. Cs3, Inc.; *The Reverse FireWall®:* Defeating DDoS Attacks Emanating from a Local Area Network; http://www.cs3-inc.com/pubs/Reverse_FireWall.pdf
5. *Defending Government Network Infrastructure Against Distributed Denial of Service Attacks;* http://www.cs3-inc.com/pubs/Defending_Govt_Network_Infrastructure.pdf

A flash based demonstration of DDoS incoming and outgoing attacks and illustrates MANAnet applied technology solutions:

Cs3, Inc. MANAnet–DDoS Demonstration

MANAnet Shield

INCOMING DDoS Defense:

MANAnet Router: a modified router implements Path Enhanced IP and fair service for packet forwarding; and

MANAnet Firewall: modified firewall implements PEIP and Fair Service in addition to rate limiting unexpected packets, and provides site-specific customizations.

OUTGOING DDoS Defense:

MANAnet Reverse Firewall™: ensures that a network can never be successfully used to initiate DDoS attacks.

It protects the internal communication of customers during an attack, whether originating from inside or outside.

Detects and notifies administrators about attack traffic from their site, so that they may take further security precautions.