Global Information Assurance Certification Paper

Deployment of New Tools by Infrastructure Owners and the Role Content Delivery Networks (CDN) Play In Combating Denial-of-Service Attacks

by Allen A. Jones November 27, 2001 --------- Security Essentials Pratical

With the assumption that readers of this document understand, at least in concept, what is a Denial of Service attack, I will skip preliminary explanations and get right to the main idea of this paper: The only way to realistically guard against Denial Of Service attacks is to take a proactive instead of reactive approach. Two of the most effective ways of preventing these types of attacks are (1) ISP implementation of anti denial-of-service tools, IP enhancement providing more accurate source address audit trail, firewall prioritization of traffic (2) and the utilization of content delivery networks.

> Peter Tippett, PhD, M.D., respected security researcher and Chief Technology Officer at ICSA.Net, emphasized the need for proactive security measures. "DDoS attacks cannot be stopped by relying on conventional, reactive technologies and security policies alone. By the time the attack has been analyzed and a response put in place, the damage has already been done," Tippett said. "Effective mitigation of the risk posed by DDoS attacks must come from adherence to generic and proactive security policies, adoption of proactive technologies designed look for hostile actions not specific signatures, and forward-thinking security planning." [1]

The responsibility for secure communications is spread over every part of the network communications path from carrier to the host; however, the ISPs need to play a much more active role since their infrastructure actually facilitates these attacks. Attackers need to have Internet access before they can connect to and then ultimately compromise a device on the Internet. This access has to come from someone. ISPs provide these "on-ramps" to the information highway. So obviously, ISPs should play a huge role in securing the Internet from hacker attacks.

> "When you [fight a DoS attack] at the end enterprise, then it's reaction. If you do it upstream from the enterprise, then it is prevention," Pescatore said.[2]

Since, ISPs own the routers and are giving attackers access to the Internet, they bare a huge responsibility in protecting their law-abiding customers from their 'hacker' customers. Any arguments that excuse ISPs from this important responsibility, in my view, is an attempt to blame or redirect attention to another part of this puzzle. Just like any business entity that provides customers a product or service, these cannot be endangering to customers or else people will not buy them. Notably, just like any business that offers a service or product, these evolve over time to meet the demands of their customers. So too, must the ISPs also evolve to incorporate more security into their networks. As ISP networks evolve with the addition of new, more powerful, feature rich equipment providing QoS over individual sessions, the task of mitigating Denial of Service attacks should become much more easier.

> Denial-of-service attacks are constantly evolving and are more automated, self-propagating and faster to deploy than ever before, according to paper authors

> Kevin Houle and George Weaver, both CERT/CC employees. A number of the most recent and high-profile worms, such as Code Red and Nimda, underscore this point, they wrote. These developments have led to a "steady increase in the ability for intruders to easily deploy large distributed denial-of-service attack networks," they wrote. Beyond automation and self-propagation, denial-of-service attacks are increasingly focusing on routers - hardware devices that help determine where traffic is sent on the Internet, according to the paper. Routers can be taken over as a result of poor configuration or administration, they wrote. Router attacks are "of extreme concern" due to "the potential of routers being used for denial-of-service attacks based on direct attacks against the routing protocols that interconnect the networks comprising the Internet," they wrote. Such an attack could potentially severely affect the travel of traffic on the Internet. "We believe this to be an eminent and real threat with a potentially high impact," Houle and Weaver wrote. Attackers are drawn to routers, according to Houle and Weaver, "because they are generally more a part of the network infrastructure than computer systems and thus may be 'safer' in the face of attacks from rival intruders."[3]

Of course, all devices connecting to the Internet should be hardened which will secure them an order of magnitude beyond the typical "out-of-the-box" configuration. However, the typical user does not have the knowledge required to accomplish this task. For instance, just having a firewall in front of a broadband, "always on" home Internet connection would be a good start. This unfortunate trend underscores the need for those providing Internet access to shoulder most of the responsibility of securing the information highway against malicious packets.

Denial of Service attacks got front-page news back in February 2001 when the following websites: Yahoo, eBay, CNN, Buy.com, Datek, E*Trade, and Amazon all went down and were not able to be used by Internet users. Not to mention, the Microsoft DoS attacks which occurred the month previous. Although the circumstances varied with each case, all resulted in the same scenario: no service.

Since these marquee companies have suffered at the hands of DoS/DDoS attacks, the industry has seen and will continue to witness new companies popping up which have developed effective, in theory, Denial of Service prevention tools. These tools are aimed at stopping Denial-of-Service attacks as close to their origins as possible before the malicious packets arrived at their targets' interface. This proactive approach makes much more sense because the attack is eliminated before it leaves its originating network. This containment of malicious packets also eases the huge burden on Intrusion Detections Systems and Firewalls which already have difficulty dealing with source address forgery of packets.

Asta, Mazu, and Arbor Networks are several new DDoS/DoS software tool companies that have similar approaches to solving this type of attack. All three vendors implement a "one, two punch" combination of packet collection and analysis as well as a packet-

filtering appliance, both of which are placed as far upstream as possible where high volume traffic exists. These hardware-based solutions monitor, aggregate, and analyze traffic flows by collecting from key routers or from direct taps into fiber or copper lines of the routing core. All three vendors suggest specific router filters to apply once a packet source of an attack is traced back to its ingress points. While all three also recommend filters, generated by their analysis appliances, the network engineer still makes the changes to the router with filters/ACLs or rate limiting. However, there needs to be great care with simply filtering out certain source IP addresses because IP spoofing would deny "legitimate" traffic coming from the same ingress router. Furthermore, rate limiting also cannot account legitimate traffic spikes, either. Conversely, Mazu Networks works to filter out only mailicious packets.

> Sophisticated heuristics ferret out ONLY the attack packets while business continues as usual.[4]

Even though all vendors above claim they create no additional load on the routers from which they collect data, only Mazu Networks solution does not require connecting directly to the router.

> They obtain data through completely passive fiber or copper splitters. Each monitor taps multiple Gigabit-Ethernet links as well as supports OC-12 speeds.[5]

Arbor and Asta Networks also claim that they do not impede performance when pulling their traffic from key routers. By using vendor specific traffic analysis services already used for provisioning and billing applications such as: Cisco Netflow® and Juniper's packet sampling technology, inspecting router data flows is moved offline or at least off of the routers CPU and onto a separate data-communications CPU. Router CPUs have enough work to do as it is already. Yet, Arbor Networks and Asta Networks "sample" just a portion of the overall traffic unlike Mazu, which "looks at" the entire traffic flow constantly.

"Most all vendors provide a canned set of Common Attack Signature Detectors as well as a component for detecting new attacks based on network traffic anomalies. However, Mazu specifically notes that once an alert of an attack has occurred, it filters malicious traffic packet-by-packet.

> Mazu focuses on keeping the majority of good traffic flowing rather than blocking valid connection requests with rate limiting or other crude router filters. Slowing down or "throttling back" traffic or turning off an interface altogether does not solve the problem and may end up locking out legitimate users or activities. [6]

TCP/IP protocol has no way to prevent attackers from forging the source IP address (aka: IP spoofing). This fundamental weakness has yet to be corrected. Ingress filtering has been one of few options in preventing malicious packets from reaching its destination; however, good packets are also filtered out since all incoming packets, good and bad,

would have the source address of the forwarding router in question. When a router strips off the layer 3 header (network/IP layer) of an incoming packet and rewrites the header with its own source address, all good and bad packets leaving this router now have the same source address. This is exactly why most ISPs that are dealing with a Denial-of-Service attack generally do not filter traffic using the offending source IP address because legitimate users are also denied service. Most sites under attack usually are left to their own devices in responding to such an attack. Being able to identify the true source of an offending packet is almost hopeless using today's versions of Internet Protocol. This has to change. The key to this change would be to provide a path within the packet of all the forwarding devices (i.e. routers/hops). Using IP addresses would take up too much space but a numbering scheme could achieve the same goal. This would take control of the source address information away from the sender that originates the packets.

There should be more work done regarding prioritizing communication within firewalls. Firewalls should be able to recognize incoming, "unexpected" packets specifically those that are not replies to the corresponding, outgoing packets. These "unexpected" packets are scheduled at a lower priority than packets that have an established connection. Yes, those packets that initiate communication (SYN) and ICMP, etc. have not yet established a two-way conversation, and so these packets would be given a lower priority. This makes sense because there is a more of a QoS issue with hosts expecting continous data transmission rather than those wanting to start a two-way conversation. The logic being that less packets need less priority than a conversation requiring more packets and consequently more bandwidth to transmit these packets. By placing these "questionable" packets in a lower priority queue, Denial-of-Service attacks would automatically be stopped without actually stopping the access just the rate at which they are allowed access to the host. This way the "all or nothing" approach of filtering out an offending source IP does not have to be used. In addition, reverse firewalling is a concept that would keep malicious packets from leaving their backyard.

In addition, startup companies have also introduced a new paradigm, called Content Distribution/Delivery Networks, developed for speeding web page loads around the globe thereby alleviating web congestion.

> "The architecture of the Internet was never designed for the type of applications we now routinely try to run over it…unless we entirely change the underpinning framework, there will always be a need for tools and services that improve the performance and reliability of the Internet." ---- Neal Goldman, The Yankee Group[7]

Thwarting denial of service attacks is simply a by-product of a content distribution/delivery network. Akamai was the first CDN.

> It was founded by world-class computer scientists at MIT who developed a set of breakthrough algorithms for intelligently routing and replicating content over a large network of distributed servers — without relying on centralized servers

typically used by Web site owners today.[8]

Like clockwork, "me-too" rivals have also come on the scene with names such as Digital Island, Mirror Image, BT ignite, Globix, Speedera Networks, st3, etc.. By replicating and caching content to geographically distributed servers, attackers loose a single point of failure in which to exploit. Interestingly enough, this architecture was designed for speeding up performance of web traffic. By pushing the content as close to the user as possible or to the "edge", *latency*, *jitter* (unpredictable, large fluctuations in latency), and bandwidth bottlenecks are minimized. This mindset was implemented in the early days of the Internet when the 80/20 rule proclaimed that 20% of the traffic crossed the backbone of the enterprise. This was when servers were placed closest to its users. Well with the advent of faster networking technologies, this rule has been flipped on its head so that 80% of LAN traffic crossed the backbone and 20% stay within its subnet. Server centralization ensued, and everyone reverted back to the data center model. The Internet obviously performs better with a distributed approach, at least at this stage in its life, than with the centralized model. Therefore, after Microsoft's DoS incident, they smartly signed on with Akamai as a customer. Content Delivery Networks provide many positives that immensely help the operational efficiency of large global, interconnecting networks.

It is painfully obvious that the Internet has been stretched beyond its initial concept and now we are reaping the penalties of this unplanned explosion of the information age. Those who designed the Internet protocols that we use today did not forsee the ease at which those, who have malicious intents, could carve up there contribution to society. Yet, hindsight is always 20/20, isn't it? The Internet has grown so quickly that making upgrades to the infrastructure can be an overwhelming task. However, one thing is for certain, those who build a better mouse trap will always get their stuff reverse engineered by the smart rodents we know as hackers. That being said, we have no choice but to take the battle to them and be proactive instead of waiting for the door to come crashing down on us unprepared. For those companies smart enough and financially capable enough to have their web content managed by a CDN, great! Nevertheless, for those that do not, infrastructure owners are there only hope to stave off these highly coordinated and automated attacks that could cost tens of thousands to billions of dollars in lost revenue. Furthermore, the infrastructure owners, logically, are the best choice for implementing tools and equipment for combating Denial-of-Service attacks since they are the only one who would able to keep these attack packets from leaving their subnet and affecting others on the WWW. Naturally, the equipment that processes these packets needs new functionality to protect the rest of the Internet from these malicious packets; the protocol itself that dictates how these packets are formed and transmitted needs an overhaul. There is not much built-in auditable information in each packet that can be traced to the originating sender. Finally, QoS technology needs to become a reality for non-ATM protocols as well as for firewalls. These carrier class features would be pushed from the backbone to the edge, on into the enterprise, and be used in a way that probably many didn't think when designing these protocols. People are not looking for tools that simply indentify mailicious packets and suggest a "plain vanilla" router filter. The companies that can identify the "attacker" packets within a myriad of "good" packets, and

successfully mitigate their ability without degrading network performance, will be the leaders of tomorrow's software environment.

---

[1] http://www.ealaddin.com/news/2000/esafe/eSafeDDOSApplets.asp
[2] http://www2.infoworld.com/articles/hn/xml/01/05/08/010508hndos.xml?Template=/storypages/printfriendly.html
[3] http://www.nwfusion.com/news/2001/1024dosattack.html
[4] http://www.mazunetworks.com/solutions.html
[5] http://www.mazunetworks.com/howitworks.html
[6] http://www.mazunetworks.com/solutions.html
[7] http://www.akamai.com/html/en/tc/tech_index.html
[8] http://akamai.com/html/en/ia/history.html