Global Information Assurance Certification Paper

Insuring Backbone Availability
Through Protecting the End-User
By: Thell B. Fowler IV

Introduction

As of July 2001 it was estimated that over 426 million individuals use the Internet, and that 236 million active users spend an average 9.5 hours online a month[1]. In the October Netcraft server survey the number of server hosting sites was just over 33 million[2]. Many people may say that protection from malicious activities is an individual's responsibility, yet when that many people are part of a community it becomes the responsibility of the leaders of that community to take up the reigns of protection for as many users as possible from those few who would wreak havoc. A simple search on general search engines (Yahoo, Google, Infoseek) would reveal guides, tutorials, and step-by-step instructions for how an end user could protect themselves, yet we already know what happens when security is left to those without any want, will, or desire to "learn" about computers.

According to Computer Economics the costs so far in 2001 from malicious code, like the Internet worms Code Red and Nimda, has risen to 11.8 billion dollars (still not beating last years 17.8 billion).[3] The frustration felt by end-users, administrators, service providers, e-based businesses, and law enforcement agencies easily matches and surpasses any monetary amount.

My goal is to spotlight some organizations and ideas that could help Internet Service Providers pave a safer and more secure Information Highway.

VISUALIZING NETWORKS

To the end user there are essentially three different types of popular connections, the dial-up connection, the digital subscriber line (DSL) connection, and the cable connection. Yes, there are others like satellite, integrated services digital network (ISDN), the various T level connections, and multiple others; yet those are being pushed out of the home user market, as well as the small office/home office market.[4]

There are several projects underway throughout the world working on visualizing the Internet. Here are a few of the great resources available for further study:

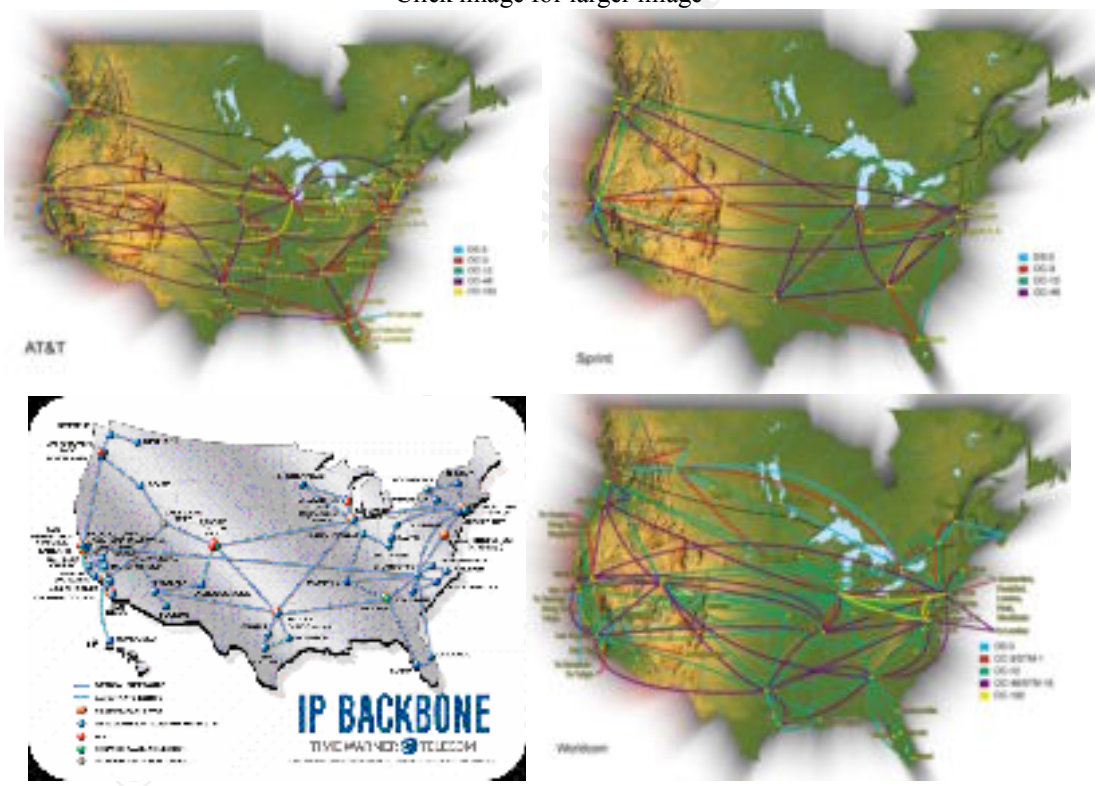
> A gallery of images along with links can be found at An Atlas of Cyberspaces, Cyber-Geography Research, Centre for Advanced Spatial Analysis (CASA), University College London.
>
> An excellent resource is CAIDA (The Cooperative Association for Internet Data Analysis). It is a conglomeration of commercial, government, and research organizations that study and analyze various Internet metrics. One portion of

these studies is Internet visualization, and there are several utilities, which can be downloaded (or even used online) to help with visualizing, like Mapnet.

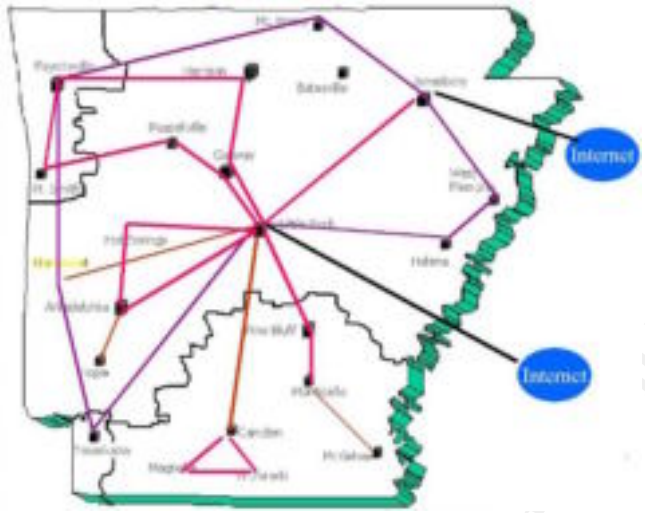
For a more detailed view of a specific service providers ISPWorld's Boardwatch might even help you find your service provider. ISPWorld gives dynamic up-to-the-minute, in depth information for numerous areas aimed at the Internet service provider community.

The following images are examples of what you can find at ISPWorld. They illustrate the national layout of the backbone for four major service providers. Backbones are the high bandwidth connections that connect the various points of presence (POP) in a network. The more users and content going across a network, the larger the pipeline needs to be. For these providers you can see the usages of DS3 (44Mbps) up to OC192 (10Gbps) are being used. (Visit the Webopedia bandwidth quick reference chart for more on line speeds.)

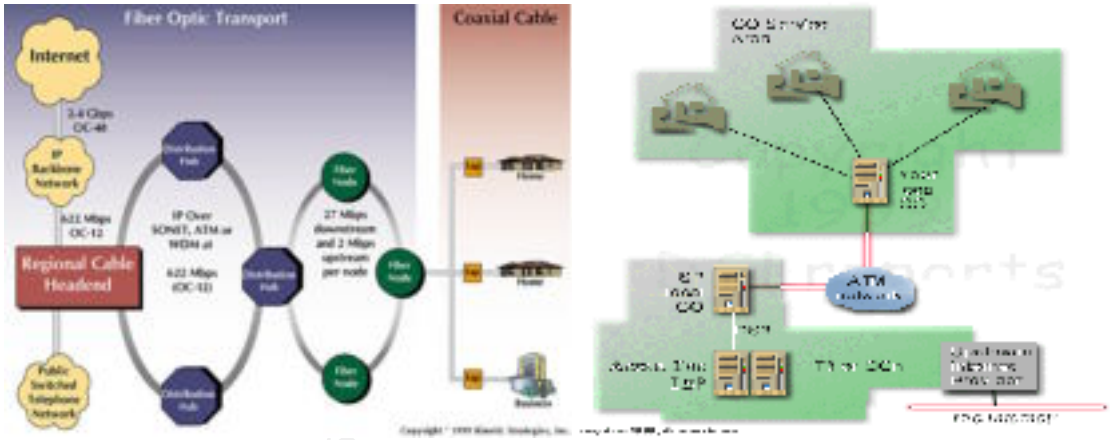
* Click image for larger image *



This macro level view rarely represents where the end-user actually connects to the Internet, so to narrow it down another layer let's view a state level map. The following is the Future Backbone Map of Arkansas. A larger image is available from the Arkansas Department of Information Systems.



This is where we start to see a break off of the various service providers to end-users. The following are examples of digital subscriber and cable networks that go directly to end-user homes and offices.



The image on the left (from Cable Datacomnews Modem Info Center diagrams page) depicts how a cable network gets the signal from the end-user to the Internet, and the image on the right (from DSLReports About DSL picture page) shows the same for a DSL customer. To learn more about how these networks particular parts work, Cable Datacom News and DSLReports both offer excellent information. If you compare the network at your neighborhood level to the networks at the state or national level, you can see that the concept of securing the infrastructure itself needs to encompass from the user up. Historically security has focused on the network down, so that a user was supposed to secure their network and not worry about the service provider, the service provider was to secure their network, and not worry about the stream between the layer above and the user, etc… Years and years ago, prior to the Internet worm invasions of 1987 and 1988 the main attack on availability was accidental denial of service attacks caused by programming or user error. Not so today, and visualizing the networks of today from the

millions of homes and offices one can see how particular networks can easily become flooded.

CURRENT ISSUES

Currently there are not very many offerings from service providers for secured access to the Internet. When an emergency arises the service providers handle the situations in a few methods. When Code Red started creating issues on the Excite@HOME cable network they reacted by blocking incoming access to port 80 (port 80 is commonly used to host web pages to the public), scanning their network and notifying owners of infected systems, as well as disconnecting non responsive system owners from the network.[5] This proves to not only be expensive and time consuming, but it is also not very effective on the whole, as can be seen with the onslaught of a newer and more advanced Internet worm named Nimda. Nimda followed on the heels, and even took advantage of changes made by, Code Red.[6] Even though the response to Nimda was quicker and more effective than the response to Code Red, it still infected over 450,000 hosts and sucked up bandwidth on service provider networks and crashed organizations local networks to such an extent that some businesses and individuals voluntarily disconnected from the Internet until they felt assured they could avoid the adverse affects. By visiting Trend Micro's Trend World Virus Tracking Center we can see Nimda variants are still creating problems worldwide.

Currently there isn't an affective way to mitigate distributed denial of service (DDoS) attacks for the non-technology inclined end-user either. These attacks make use of the ignorance of end-users and insecure coding practices, both in penetrating and installing the attack tools as well as performing the attack. DDoS attacks are taking place constantly on the Internet at an amazing rate. Recently a research method known as backscatter analysis was created that helps in quantifying information dealing with DDoS attacks.[7] From section 6 of the abstract on this method:

> "…we observed 12,805 attacks over the course of a week. Table 2 summarizes this data, showing more than 5,000 distinct victim IP addresses in more than 2,000 distinct DNS domains."

The research paper goes further into classifying the attack method, attack rates, and victim identification, by analyzing the unsolicited responses produced by victims responding to spoofed attack packets.

There are several dynamically updated 'Internet Weather/Traffic' maps on the Internet to get a feel for what is happening throughout the world.

> DShield, Distributed Intrusion Detection System, keeps a global map with pie graphs indicating the most attacked port, and the top attacker IP address. They provide client programs for users of firewalls to share data regarding attack information. If you use a firewall *please* get involved with this program.

The Internet Weather Report from Matrix.net has various geographical maps showing ping response times (latency) from their office in Austin, TX to thousands of hosts around the world, along with historical data.

The Internet Traffic Report updates ping times to routers every 15 minutes and then assigns a 'traffic index' number. Allowing you to drill down from a global perspective to an individual routers history. This site allows network administrators to include their own routers to help make the report more accurate and useful.

Another ongoing plague for end-users that affects the whole of the Internet (and propagates malicious programs) is unchecked email activity. Even though a lot of work has gone into insuring the privacy of email, the responsibility still resides with the end-user to make sure that they don't open unsolicited attachments without scanning them. Once again, we can see how ineffective this is by looking at how long SirCam and LoveLetter have remained at the top of the virus activity lists. SirCam, a Trojan horse program has been consistently been #1 and hasn't fallen out of the Top 5 since it was originally discovered July 18, 2001. LoveLetter, and its' variants, come as a virus and then (in some versions) attempt to download a password stealing Trojan; since it debuted in May of 2000 it is still on the Trend Micro Real-Time Top 10.

POSSIBLE SOLUTIONS

There is the possibility to circumvent the spreading of these activities and to bring the perpetrators to justice through the cooperation of hardware manufacturers and service providers which in turn will provide enforcement agencies with more substantial and factual information to prosecute.

Home users have, for quite some time, had access to products like the Linksys Cable/DSL Switch, for home security. Usually, someone 'in-the-know' will inform the user once they start to have issues or problems with security, and then they will begin to look into solutions like this. The future of creating network solutions that won't require end-user activity like that looks promising.

The engineers at companies like Cisco and Ericsson have taken security a step in the right direction by making the cable modem itself the security device and taking the security out of the hands of end users. The Ericsson PipeRider Enhanced Security Cable Modem HM204c has Safe@Home firewall software based on Checkpoint's Firewall-1 technology. This cable modem allows the service provider operator to manage the security services and updates remotely. As companies like Time Warner (Time Warner sign deals with Ericsson[8]) begin to take advantage of these types of modems and offer service packages that are in-line with the end-users abilities, security of our infrastructure begins to become a reality. By creating account offerings that make the least expensive accounts the most secure and then offering a version of that same account that has more flexibility cost more, the service provider decreases security related losses, increases revenues, and increases security at the same time. Add to that scanning of incoming and

outgoing email for known malicious code signatures and hopefully future releases of products that also allow for ingress/egress filtering (to stop spoofed transmissions within their network) and the backbone availability becomes much more secure.

Service providers, who have educated administrators and proper policies, should already be taking advantage of best practices as set forth for their environment and systems[9]. The addition of future router design and specifications that utilize router stamping[10] in conjunction with traffic analysis systems could also be implemented. Router stamping is proposed as a method of identifying the source location of spoofed packets through the use modifying header information to store the routers a packet passes through.

For example, the utilization of the backscatter techniques mentioned previously along with router stamping allows for a real time analysis to be done across the Internet backbone. In the future a DDoS attack could be initiated much like it is now when a coordinated attack is used, yet with the cooperation and cross referencing of data from each major provider with direct access to the backbone the data from an automated backscatter analysis could quickly and accurately diagnose a signature and cross apply it, thereby keeping the backbone itself protected. The only damage incurred would be on the internal networks of the service providers sending the information. This would be an externally focused protection mechanism.

Another step in helping to insure that the people who would try to cripple the Internet are brought to justice is the automatic submission of router reports to projects such as DShield. By having multiple service providers cross referencing the IP information of attack addresses, along with the report records of routers with stamping capability, and lastly the reports created by the management software securing broadband connection modems there would be logs of any and all malicious activity. If this activity is coming from an account that was paying for higher 'flexibility' then automated downgrading of the account could be done until enforcement agencies decided what to do.

Let's see how a solution like this would be able to handle an attack like Nimda that utilizes multiple methods to propagate.[11]

1. The first attack method being an email attack. Included in the MIME header is the Content-Type: audio/x-wav; name="readme.exe". As soon as this email is viewed on a non-secured client Nimda it will begin to spawn multiple threads within that system and go through the process of making the needed changes to insure its' control. Then it will begin to attack the local network.

This method of attack could be handled by holding both incoming and outgoing email for scanning for a short period of time. When a massive influx of email is noted to have the same signatures (the hostility of the email is unknown at this point); then it continues to hold them and sends an alert to an administrator. In this case, when the administrator does indeed diagnose the malicious code the signature is downloaded to the local email scanning system. (There are several email protection programs available for this influx/bombing type protection available already, like Sophos) At this point there is still

traffic on the internal end-user network of emails being sent; that is stopped as soon as the cable/DSL modem equipped with an auto-update scanning protection mechanism downloads that signature to itself. This stops the flow those outgoing messages before they can even get started.

2. Nimda will attack any available drive shares, copying itself to these locations and beginning execution. Any .htm, .html, .asp pages it finds will be changed so that it will continue to spread via web access as well.

This second method of attack is a common problem on some peer based cable/DSL networks since so many end-users do not have any idea if the shares are on; or even what a share is! By utilizing a firewall equipped cable/DSL modem the most basic account type would have zero open ports to the outside and no capacity to share the drive outside of their home network; much like a totally locked down firewall would do now. Once again the service providers bandwidth is protected from internal scans and wasted bandwidth.

3. The last style of propagation is modification of files. Both the files that are used for running the system (.dll and .exe files) as well as files that would be browsed by external users (.htm/.html/.asp). This allows for the spread of the virus through servers.

Most end-users do not have permission to run servers; most don't even know that they are running services available externally. Once again the firewall portion of the cable/DSL modem enforces the agreement policy prior to any bandwidth being used!

4. The insertion of malicious code like Nimda would typically be done using spoofed IP information, and during an actually DDoS portion of an attack on a specific target the use of a spoofed IP would usually be used as well.

The use of ingress/egress filtering both within the cable/DSL modem and the service provider's routers would alleviate this type of attack.

5. Lastly, an attack like that of Nimda becomes widespread in our current environment so quickly that backtracking to any one particular source becomes virtually impossible.

The use of router stamping for all service providers, along with backscatter analysis, and forecasting projects such as Predictor or HoneyNet[12] would give quick and accurate pinpointing of the initial release network. The logs from that network (if using best practices would be able to pinpoint a particular IP along with subsequent results to forward to enforcement agencies.

CONCLUSION

The backbone of the Internet is vital to protect, and with the burgeoning of new always-on broadband connections it is imperative that externally focused security methods

become a standard. Protecting the rest of the Internet from those who innocently leave the doors and windows open is the responsibility of each of us who know the risks. The outlook is bright that our future will have policies that take advantage of hardware and software solutions that focus on these vulnerabilities in an effective and accomplishable fashion. Each of us has our part to do, and I once again urge you to join one of the many projects that are ongoing in network traffic analysis, as well as emailing your local service provider and sound out on behalf of these technologies.

The focus on insuring availability of services has changed dramatically over the years; I'd like to finish with two quotes that emphasize this:

> "In cases where denial of service attacks did occur, it was either by accident or relatively easy to figure out who was responsible. The individual could be disciplined outside the operating system by other means." ~ Dennis Ritchie[13]

> "What is interesting about solutions dealing with DDoS is that they require the cooperation of many different parties." ~ Aviel D. Rubin[14]

---

[1] Michael Pastore 426 Million Online Worldwide (11 June 2001)
http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_782281,00.html (19 Nov. 2001)

[2] Netcraft Web Server Survey (Oct. 2001)
http://www.netcraft.com/survey/ (19 Nov. 2001)

[3] Beverly Waite Computer Economics Cyber Quake Index (26 Sept. 2001)
http://www.computereconomics.com/cei/press/pr92101.html (19 Nov. 2001)

[4] Michael Pastore Growing Broadband Market Could Lift Economy (16 July 2001)
http://cyberatlas.internet.com/markets/broadband/article/0,,10099_802141,00.html (19 Nov. 2001)

[5] AT&T Broadband. What Do I Need To Know About The Code Red Virus (7 Aug. 2001)
http://help.broadband.att.com/faq.jsp?content_id=792&category_id=19 (19 Nov. 2001)

[6] Incidents.org / Sans Institute. NIMDA Worm/Virus Report – Final PDF Document (3 Oct. 2001)
http://www.incidents.org/react/nimda.pdf (19 Nov. 2001)

[7] David Moore, Geoffrey Voelker, and Stefan Savage. Inferring Internet Denial-of-Service Activity (4 Oct. 2001)
http://www.caida.org/outreach/papers/backscatter/index.xml (19 Nov. 2001)

[8] Press Release. Time Warner Selects Ericsson cable modems (11 Jan. 2001)
http://www.ericsson.com/infocenter/news/time_warner.html (19 Nov. 2001)

[9] Carnegie Mellon University CERT Security Improvement Modules Practices (18 Oct. 2001)
http://www.cert.org/security-improvement/#practices (19 Nov. 2001)

[10] Thomas W. Doeppner, Philip N. Klein, Andrew Koyfman. Using Router Stamping to Identify the Source of IP Packets Athens, Greece ACM Press, 2000

[11] Andrew Mackie, Jensenne Rockulan, Ryan Russell, Mario Van Velzen. Nimda Worm Analysis Aris Predictor Incident Analysis Report Version 2, (21 Sept. 2001)

http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf (19 Nov. 2001)

[12] Honeynet Project. Know Your Enemy: Statistics (22 July 2001)
http://project.honeynet.org/papers/stats/

[13] Simson Garfinkel and Gene Spafford Practical Unix & Internet Security 2nd Edition Sebastopol, CA O'Reilly & Associates, Inc., April 1996 Pg. 759

[14] Aviel D. Rubin. White-Hat Security Arsenal Upper Saddle River, NJ Addison-Wesly, 2001. Section 11.2.4 paragraph 3