

Network Security – Defense Against DoS/DDoS Attacks

Hang Chau

Abstract

DoS/DDoS attacks are a virulent, relatively new type of Internet attacks, they have caused some biggest web sites on the world -- owned by the most famous E-Commerce companies such as Yahoo, eBay, Amazon -- became inaccessible to customers, partners, and users, the financial losses are very huge. On the other hand, if the international terrorist organizations use the DoS/DDoS to attack successfully the web sites or Internet systems of U.S. government and military, the results and losses will be disastrous and unimaginable. Therefore, for guarding both American national security and commercial security, it is really important to detecting, preventing and mitigating the DoS/DDoS attacks.

1. Introduction

DoS/DDoS attacks are a virulent, relatively new type of Internet attacks, they have caused some biggest web sites on the world -- owned by the most famous E-Commerce companies such as Yahoo, eBay, Amazon -- became inaccessible to customers, partners, and users, sometimes for up to twenty-four hours; some web sites have experienced several days of downtime while trying to restore services, the financial losses are very huge.

From a latest important report “**2003: CSI/FBI [1] Computer Crime and Security Survey**”, we know the following information about the DoS/DDoS attacks in America:

1. 42 percent of respondents of the survey suffered the Denial of Service (DoS) attacks (from 1999 to 2002, only 27-40 percent of respondents suffered the DoS attacks).
2. 111 of 398 respondents reported the financial losses caused by the DoS attacks.
3. The total losses by DoS attacks was over 65 million US dollars, or average losses 1.427 million dollars, it is the 4.8 times of average losses on 2002 (from 2000 to 2002, the average losses caused by the DoS attacks are only 0.108, 0.122, 0.297 million dollars respectively).
4. In “WWW Site Incidents: What Types of Unauthorized Access or Misuse”, 35% are Denial of Service attacks.
5. In addition, on the 2001’s version of the CSI/FBI Survey, when the DoS attacks increased by an astonishing 33 percent on network, where firewalls had been installed in 90 percent of instances.

DoS/DDoS attacks are also easy to launch. For example, a teenager using very simple DoS tools managed to cripple the web sites of large E-Commerce companies like Yahoo and Amazon, during a series of DoS/DDoS attacks in February 2000 [2].

On the other hand, we must think more and far. If the international terrorist organizations use the DoS/DDoS methods to attack successfully the web sites or Internet systems of U.S. government and military, the results and losses will be disastrous and unimaginable. Therefore, for guarding both American national security and commercial security, it is really important to detecting, preventing and mitigating the DoS/DDoS attacks.

2 The Protection Act against DDS (DDoS) Attacks

The DoS/DDoS attacks are virulent and very hateful, so they are never joking matter. In the U.S., the attacks can be a serious federal crime under the **National Information Infrastructure Protection Act of 1996** [3] with penalties that include years of imprisonment, many other countries also have similar laws. The U.S. Department of Justice and other federal agencies are continually working to better prevent computer crimes and enforce existing laws concerning computer crime.

In the **Computer Crime and Intellectual Property Section (CCIPS)** of the U.S. Department of Justice, we can find:

Item B – National Information Infrastructure Protection Act of 1996, it was enacted as part of Public Law 104-294. It amended the Computer Fraud and Abuse Act, which is codified at 18 U.S.C. § 1030.

Item C – Distributed Denial of Service Attacks, it wrote: “In the week of February 7, 2000, hackers launched distributed denial of service (DDoS) attacks on several prominent websites, including Yahoo!, E*Trade, Amazon.com and eBay. In a DDoS attack, dozens or even hundreds of computers all linked to the Internet are instructed by a rogue program to bombard the target site with nonsense data. This bombardment soon causes the target sites’s servers to run out of memory, and thus cause it to be unresponsive to the queries of legitimate customers. On February 29, 2000, Deputy Attorney General Eric Holder and Director of the National Infrastructure Protection Center Michael A. Vatis testified before a House and Senate Joint Judiciary Subcommittee meeting to talk about the distributed denial of services attacks and about cybercrime in general. ...”

3. DoS Attacks and Defense Against the Attacks

3.1 Overview

What’s DoS (Denial of Service, also known as “nuke”, “hacking”, or “cyber-attacks”) attack? A DoS attack is an attempt to prevent legitimate users of a service or network resource from accessing that service or resource. DoS attacks usually make use of software bugs to crash or freeze a service or network resource, or bandwidth limits by making use of a flood attack to saturate all bandwidth.

3.2 DoS Attack Methods

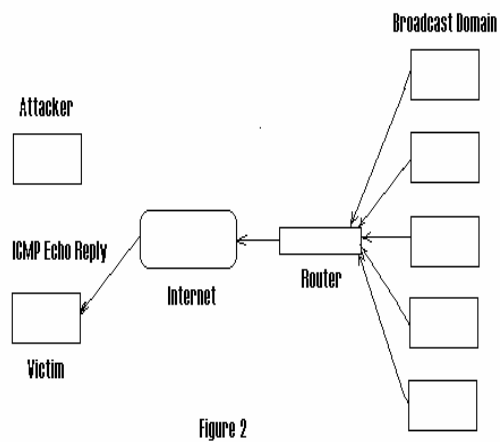
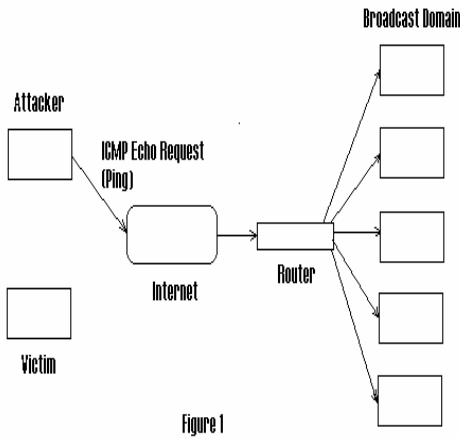
There are three generic DoS attack methods stand out as particularly dangerous:

Smurf or Fraggle

Smurf attacks are one of the most devastating DoS attacks. See the Figure 1, in the Smurf (ICMP Packet Magnification) attack, the attacker sends an ICMP echo request (ping) to a broadcast address. The source address of the echo request is the IP address of the victim (uses the IP address of the victim as the return address). After receiving the echo request, all the machines in the broadcast domain send echo replies (responses) to the victim’s IP address (see the Figure 2). Victim will be crash or freeze when receiving larger-sized packet flood from many machines.

Smurf attack uses bandwidth consumption to disable a victim system’s network resources. It accomplishes the consumption using amplification of the attackers bandwidth. If the amplifying network has 100 machines, the signal can be amplified 100 times, so the attacker with relatively low

bandwidth (such as the 56K modem) can flood and disable a victim system with much higher bandwidth (such as the T1 connection).

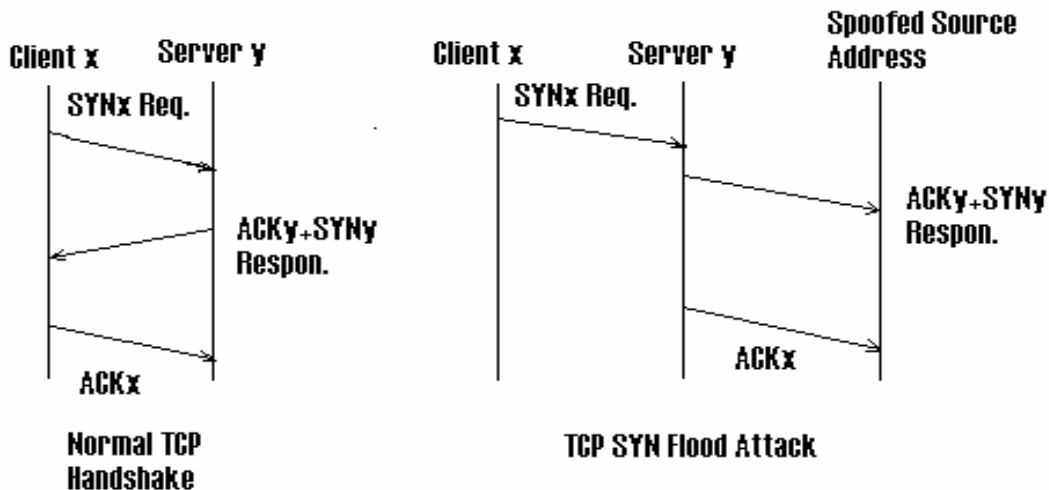


The Fraggle (UDP Packet Magnification) attack is the cousin of Smurf attack. Fraggle attack uses UDP echo packets in the same fashion as the ICMP echo packets in Smurf attack. Fraggle usually achieves a smaller amplification factor than Smurf, and UDP echo is a less important service in most network than ICMP echo, so Fraggle is much less popular than Smurf.

SYN Flood

The SYN flood attack was considered to be the most devastating DoS attack method before the Smurf was discovered. This method uses resource starvation to achieve the DoS attack.

See the figure on below, during a normal TCP handshake, a client sends a SYN request to the server; then the server responds with a ACK/SYN to the client, finally the client sends a final ACK back to the server.



But in a SYN flood attack, the attacker sends multiple SYN requests to the victim server with spoofed source addresses for the return address. The spoofed addresses are nonexistent on network. The victim server then responds with an ACK/ SYN back to the nonexistent address. Because no address receives this ACK/SYN, the victim server just waits for the ACK from the client. The ACK

never arrives, and the victim server eventually times out. If the attacker sends SYN requests often enough, the victim server's available resources for setting up a connection will be consumed waiting for these bogus ACKs. These resources are usually low in number, so relatively few bogus SYN requests can create a DoS event.

DNS Attacks

On earlier versions of BIND (Berkeley Internet Name Domain), attackers could effectively poison the cache on a DNS server that was using recursion to look up a zone not served by the name server. Once the cache was poisoned, a potential legitimate user would be directed to the attacker's network or a nonexistent network. This problem has been corrected with later versions of BIND.

3.3 Defensive Technologies

3.3.1 Defense Against Smurf or Fraggle Attacks

If you find yourself the target of a Smurf attack, there is unfortunately not much you can do. Though it is possible to block the offending packets at your external router, the bandwidth upstream of that router will remain blocked. It takes coordination with your upstream network provider to block the attacks at the source.

To prevent someone at your site from initiating a Smurf attack, configure your external router to block all outbound packets from your site that indicate a source address not contained within your subnet block. If the spoofed packet can't get out, it can't do much harm.

To avoid being an intermediary, and contributing to somebody else's Denial of Service attempt, configure your router to block all network-prefix-directed broadcast packets. That is, disallow broadcast ICMP packets in through your router. This will allow you to retain the ability to perform a broadcast-directed ping inside your network, while eliminating an outsider's ability to exploit this behavior. If you are truly worried, you may also wish to configure your host machines to ignore ICMP broadcasts entirely.

3.3.2 Defense Against SYN Flood Attacks

Micro Blocks

Instead of allocating a complete connection object (which causes the memory failure), simply allocate a micro-record. Newer implementations allocate as little as 16-bytes for the incoming SYN object.

SYN Cookies

A new defense against SYN flood is "SYN cookies". In the SYN cookies, each side of a connection has its own sequence-number. In response to a SYN, the attacked machine creates a special sequence number that is a "cookie" (cookie is used as unique identifier of a negotiation exchange) of the connection then forgets everything. It knows about the connection. It can then recreate the forgotten information about the connection when the next packets come in from a legitimate connection.

RST Cookies

It is an alternative to SYN cookies, but may cause problems with Win95 machines and/or machines behind the firewalls. The way this works is that the server sends a wrong ACK/SYN back to the

client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will accept incoming connections from that client normally.

Stack Tweaking

TCP stacks can be tweaked in order to reduce the effect of SYN floods. The most common example is to reduce the timeout before a stack frees up the memory allocated for a connection. Another technique would be to selectively drop incoming connections.

3.3.3 Defense against DNS attacks

Defending the root server

The root server database is small and changes infrequently, download an entire copy of the root database, check for updates once a day, and stay current with occasional reloads. Deploy root servers using “anycast” addresses that allow multiple machines in different network locations to look like a single server.

Defending your organization

If your organization has an intranet, you should provide separate views of DNS to your internal users and your external customers. This will isolate the internal DNS from external attacks. Copy the root zone to insulate your organization from future DDoS attacks on the root. Consider also copying DNS zones from business partners on extranets. When DNS updates go over the Internet, they can also be hijacked in transit – use TSIGs (transaction signature) to sign them or send updates over VPNs or other channels.

4. DDoS Attacks and Defense Against the Attacks

4.1 Overview

DDoS attack is a large-scale, coordinated attack on the availability of Internet services and resources. It launches indirectly the DoS attacks through many compromised computers (they often are called “secondary victims”). The Internet services and resources under the attack are “primary victims”. DDoS attack is generally more effective to bring down huge corporate sites than DoS attacks. A typical DDoS attack consists of master, slave, and victim – master being the attacker, slave being the compromised systems and victim of course being the attacker’s target.

4.2 The Types of DDoS Attacks

Generally, DDoS attacks are a combination of four types: Trinoo, TFN, TFN2K, Stecheldraht.

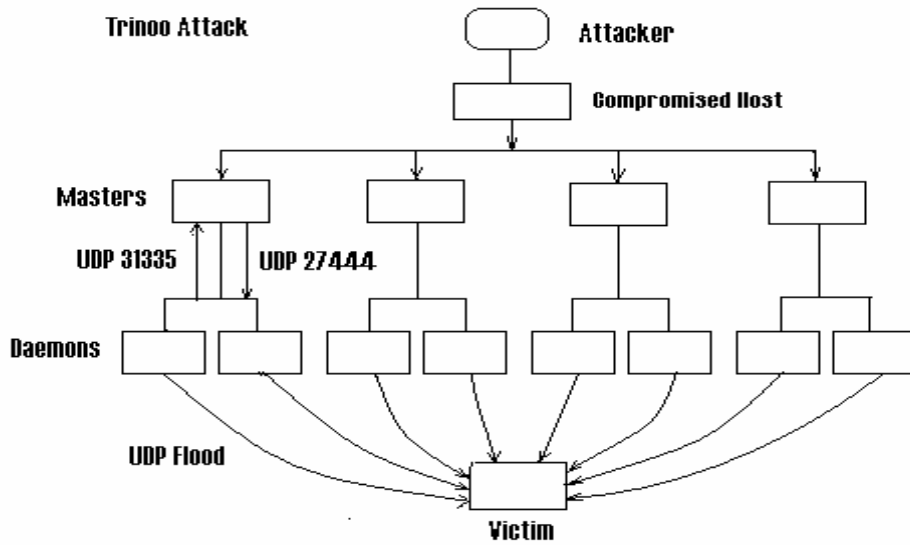
Trinoo

Trinoo is essentially a master/slave (called Masters and Daemons) programs that coordinate with each other to launch a UDP DoS flood against a victim machine.

See the figure, in a typical scenario, the following steps take place as the Trinoo DDoS network is set up:

Step 1 The attacker, using a compromised host, compiles a list of machines that can be

compromised. Most of this process is done automatically from the compromised host, because the host stores a mount of information including how to find other hosts to compromise.

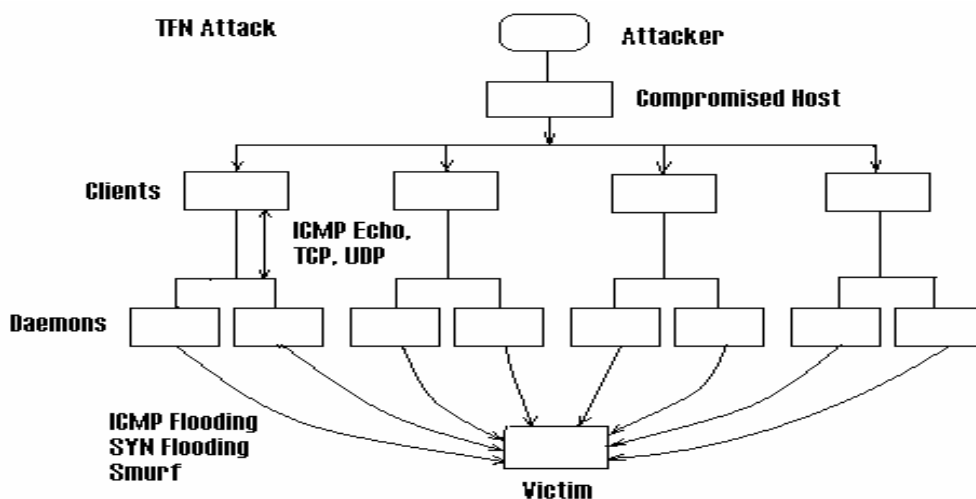


Step 2 As soon as the list of machines that can be compromised has been compiled, scripts are run to compromise them and convert them into the Trinoo Masters or Daemons. One Master can control multiple Daemons. The Daemons are the compromised hosts that launch the actual UDP floods against the victim machine.

Step 3 The DDoS attack is launched when the attacker issues a command on the Master hosts. The Masters instruct every Daemon to start a DoS attack against the IP address specified in the command, many DoSs compromise the DDoS attack.

TFN/TFN2K

TFN (Tribal Flood Network), like Trinoo, is essentially a master/slave (called Clients and



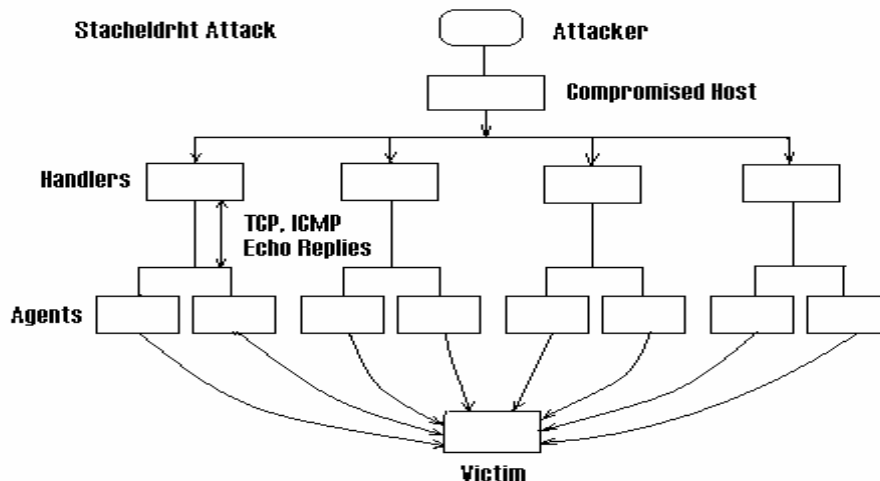
Daemons) programs that coordinate with each other to launch a SYN flood against a victim machine, see the figure. The TFN Daemons, however, are capable of a larger variety of attacks,

including ICMP flooding, SYN flooding, and Smurf attacks, so TFN attack is more complicated than the Trinoo attack.

TFN2K introduces some enhancements to the original TFN tool. TFN2K attacks are launched using spoofed IP addresses, making detecting the source of the attacks more difficult. TFN2K attacks are not just simple floods like those in TFN. They also include attacks exploiting the operating system’s vulnerabilities to malformed or invalid packets, which can cause the victim machines to crash. The TFN2K attackers no longer need to execute commands by logging into the Client machine, they can execute these commands remotely. The communication between the Clients and the Daemons is no longer limited to simply ICMP echo replies, it can take place over a larger variety of mediums, such as TCP and UDP. So TFN2K attacks are more dangerous and also more difficult to detect.

Stacheldraht

Stacheldraht code is very similar to the Trinoo and TFN, but Stacheldraht allows the communication between the attacker and the Masters (called Handlers, see the figure) to be encrypted; the Agents can upgrade their code automatically, can launch different types of attacks such as ICMP floods, UDP floods and SYN floods.



4.3 General Defensive Practices

If you are a **UNIX** or **Linux** administrator, the following basic UNIX administration practices should be followed:

1. Follow R.U.N.S.A.F.E. guidelines:
 - R**efuse to Run Unknown Programs;
 - U**ppdate Our Computers Regularly;
 - N**ullify Unneeded Risks;
 - S**afeguard Our Identity and Password;
 - A**ssure Sufficient Resources for Proper System Care;
 - F**ace Insecurity;
 - E**verybody Needs to Do Their Part.

2. Download and run test programs from the National Infrastructure Protection Center to test for the most common DDoS attack tools on Sun or Linux boxes.

If you are a **Windows** administrator, the following basic Windows operating precautions should be followed:

Follow R.U.N.S.A.F.E. guidelines (see above).

These practices and precautions will help your systems from being used in the DDoS attacks.

5. Some Further Discussions

Since the victims of the DDoS attacks usually cannot trace back to the attacker, there is a question of which other parties may be liable in terms of contributory negligence. Since some DDoS attacks can be traced back to the secondary victims, can the owners or corporations responsible for secondary victim computers be held liable for participating in an attack? Are software vendors liable for vulnerabilities in their code? Are hardware vendors responsible for not providing defenses against malicious intrusion and use of the machines they sell by remote parties other than the owners? Do network providers have an obligation to prevent their networks from allowing secondary victims to send DDoS packet traffic into the network?

One of the most important issues that will impact how defenses against DDoS attacks are deployed will be the cost of solutions and preventive measures. If DDoS prevention strategies cost companies and individuals huge sums of money, you will not see quick or wide scale deployment. It will take time before industry and government agencies buy new products. Additionally, attackers build methods to counter specific security measures. This leads to a cyclical pattern of new security systems being deployed, and new attacks being designed.

6. Some Main Vendors and Their Products

(Disclaimer: I list the vendors and their products, it does not imply I say these products are or are not good solutions. I list the vendors because they simply claim to have some kind of “solution” to the DDoS attack, or they claim the products help to protect from the attacks for enterprise-class or large network infrastructures).

6.1 Network Level Defense

Arbor’s Network: “Arbor’s network anomaly detection solutions enable the operators of large, complex networks to eliminate DDoS attacks, worms, router attacks, instability, policy violations, and other anomalous behavior.”

(<http://www.arbornetworks.com/>)

Mazu Networks: “provides enterprise-class security solutions that protect the large and complex networks operated by global corporations and major government agencies.”

(<http://www.mazunetworks.com/>)

Captus Networks: “The Captus IPS solution automatically mitigates a broad range of network intrusions including DDoS attacks, port scans, and exploits from unknown worms.”

(<http://www.captusnetworks.com/>)

CS3: “CS3’s patent-pending MANAnet Shield is a family of products and technologies that provide comprehensive, infrastructure-level defenses against both incoming and outgoing packet-flooding Distributed Denial of Service (DDoS) attacks on the Internet. MANAnet Shield incorporates both active, inline solutions and passive, off-line solutions.”

(<http://www.cs3-inc.com/>)

Riverhead Networks: “Using Riverhead’s Centralized Protection architecture, service providers can provide global DDoS protection by long-diverting suspected attack traffic from any peering point to a centralized Guard, where attack flows are removed and legitimate transactions forwarded to their original destination.”

(<http://www.riverhead.com/>)

Net Zentry: “netZentry’s first product offering, FloodGuard^(TM), locally detects and globally mitigates crippling packet floods caused by distributed denial-of-service attacks (DDoS) and zero-day worms.”

(<http://www.netzentry.com/>)

6.2 Host Level Defense

McAfee Network: “McAfee Network Protection Solutions help assure the availability and security of your network infrastructure, featuring best-of-breed products including Sniffer Technologies for network management, McAfee IntruShield for network intrusion prevention, and InfiniStream Security Forensics for network security forensics.”

(<http://www.networkassociates.com/us/products/sniffer/home.asp>)

Tripwire: “The single greatest risk to the security and stability of IT operations is undetected change to servers and network devices. Tripwire Integrity Management software helps you effectively control change—enabling you to instill process accountability, improve security, and ensure system availability.”

(<http://www.tripwire.com/>)

6.3 Augmented Intrusion Detection

Oneka: “The SAFE Blueprint uses all the security technologies... Ingress and egress filtering ... restricts outbound access from infected servers and inbound infection attempts against user systems. Using firewalls protect both the user and server segments in addition to the filtering and provides DDoS connection rate limiting for the public servers...”

(<http://www.okena.com/>)

6.4 Managed Security Services

TrustWave: “...Intrusion Protection Systems offer identical capabilities as IDS with the added benefit of actively protecting a client’s network without the need of signature updates. Intrusion Protection Systems install the Cisco Security Agent (CSA) onto desktop and server resources which act as gateways to protected activities such as accessing privileged functions of the operating system or sending email...”

(<http://www.trustwave.com/>)

Solsoft: “Solsoft offers a breakthrough to network security. The technology makes it possible to design and apply policy on a ‘virtual network’ without constraints from device brands and capabilities”.

(<http://www.solsoft.com/pages/home/home.php>)

Aprisma: “Aprisma’s SPECTRUM software manages the health and performance of networks – and the business services that rely on them... SPECTRUM can automatically discover and understand the relationships between network infrastructure elements, services and customers... Intelligently isolates problems to the root cause...”

(<http://www.aprisma.com/>)

6.5 Work in Progress Research

Stottler Henke: “Aurora™ is a sophisticated scheduling system that combines a variety of scheduling techniques, intelligent conflict resolution, and decision support to make scheduling fasted and easier.”

(<http://www.shai.com/>)

7. Notes

[1] CSI: Computer Security Institute.

[2] Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice:

<http://usdoj.gov/criminal/cybercrime/compcrime.html>

and CNN article:

<http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html>

[3] The National Information Infrastructure Protection Act:

<http://www.usdoj.gov/criminal/cybercrime/ccpolicy.html#NIFPA>

8. References

Distributed Denial of Service (DDoS) Attacks/tools, University of Washington, see:

<http://staff.washington.edu/dittrich/misc/ddos/>

Distributed Denial of Service (DDOS) Attacks, James Madison University, see:

<http://www.jmu.edu/computing/info-security/engineering/issues/ddos.shtml>

Denial of Service or “Nuke” Attacks, IRChelp.org, Internet Relay Chat (IRC) help archive, see:

<http://www.irchelp.org/irchelp/nuke/>

Intrusion Detection Systems FAQ, WindowSecurity.com, see:

http://www.windowsecurity.com/articles/Intrusion_Detection_FAQ.html

Magnification Attacks: Smurf, Fraggle, and Others, pintday.org, see:

<http://pintday.org/whitepapers/dos-smurf.shtml>

SYN flood, Internet Security System (ISS), see:

http://www.iss.net/security_center/advice/Exploits/TCP/SYN_flood/default.htm

Whiter Paper: Next Generation Intrusion Detection Systems (IDS), Network Associates, see:
<http://www.mcafeesecurity.com>

CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, see:
http://www.cert.org/tech_tips/denial_of_service.html

Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice, see:
<http://usdoj.gov/criminal/cybercrime/comprcrime.html>

The National Information Infrastructure Protection Act, the Department of Justice, see:
<http://www.usdoj.gov/criminal/cybercrime/ccpolicy.html#NIFPA>

Cyber-attacks batter Web heavyweights, CNN News, see:
<http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html>

Denial of Service Attacks – DDOS, SMURF, FRAGGLE, TRINOO, iINFOSYSSEC, see:
<http://www.infosyssec.com/infosyssec/secdos1.htm>

Cisco Secure Intrusion Detection System, Author: Earl Carter; Issued: October 2001; Publisher: Cisco Press, 1st edition; ISBN: 158705034X.

Network Security Principles and Practice, Author: Saadat Malik; Issued: November 15, 2002; Publisher: Cisco Press, 1st edition; ISBN: 1587050250.

Security+ Study Guide and DVD Training System, Authors: Robert J. Shimonski etc.; Issued: December, 2002; Publisher: Syngress; ISBN: 1931836728.

=====

Hang Chau
Senior Network/System Administrator, Ming Plaza Development
hcdanny@yahoo.com
(909)864-9456
28925 Clear Spring Lane, Highland, CA 92346, U.S.A.

Degree and IT Certifications:

M.S. on Computer Science, California State University, Fresno, California, USA;

- CCIE, CCNP, CCNA (Cisco/CCIE: passed the Qualification Exam);
- SCSA, SCNA (Sun/Solaris 8: Certified System and Network Administrators);
- SCJP, SCWCD (Sun/Java 2: Certified Programmer and Web Component Developer);
- MCSE, MCSA (Microsoft 2000 Certified System Engineer and System Administrator).

Also research on Network Attacks and Network Security:

- Cisco IDS/Secure PIX (Intrusion Detection Systems and Firewall);
- DoS/DDoS (Denial of Service/Distributed Denial of Service);
- Mydoom/Doomjuice Worms and DoS/DDoS attacks.