A Controlled Environment for Study of Burst High Bandwidth Attack

XIN WANG, BINXING FANG, XIAOCHUN YUN
Research Center of Computer Network and Information Security Technology,
Harbin Institute of Technology of China, Harbin 150001, China

Abstract ∴- The current Internet infrastructure has very few built-in protection mechanisms and is therefore vulnerable to attacks and failures. The Denial of Service attack, especially the burst high bandwidth attack, has become one of the major threats to the Internet. A controlled environment for analysis and defense of orchestrated attacks similar to those in the wild is a necessary first step in their prevention. In this paper, we present a controlled environment for generation, control and surveillance of burst high bandwidth attacks.

Key-word: - Burst high bandwidth attack Control environment Denial of service

1 Introduction

A denial of service (DoS) attack is a malicious attempt by a single person or a group of people to cripple an online service. The impact of these attacks can vary from minor inconvenience to users of a website, to serious financial losses for companies that rely on their on-line availability to do business. Recently DoS attacks represent an ever increasing, ever changing threat to productivity and profitability on the Internet. Therein the type of DoS attack that causes problems by overloading the victim with massive useless traffic volume is known as a burst high bandwidth attack.

Mostly of burst high bandwidth attack rapidly evolving and increasingly aggressive nature, it has proved particularly difficult to defend against. At present, there are no effective means of protecting burst high bandwidths attacks due to the following reasons. Both IP and TCP can be misused as dangerous weapons quite easily. Since all Web traffic is TCP/IP based, attackers can release their malicious packets on the Internet without being conspicuous or easily traceable. It is the sheer volume of all packets that poses a threat rather than the characteristics of individual packets. A bandwidth attack solution is, therefore, more complex than a straightforward filter in a router. A key problem to take when solving bandwidth attacks is attack detection. Detection of a bandwidth attack might be easy in the vicinity of the victim, but becomes more difficult as the distance to the victim increases. The underlying reason is that most bandwidth attacks are launched from distributed sources. This means that the attack traffic is spread across multiple links, which makes it more diffuse and harder to detect. Most of the existing solutions [3-9] to bandwidth attacks become less effective when the attack traffic becomes distributed.

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) has been conducting the Distributed Denial of Service Defense Attack Tradeoff Analysis (DDOS-DATA). DDOS-DATA's goal is to analyze Distributed Denial of Service (DDOS) attacks and mitigation technologies. With this insight, a controlled environment for analysis and monitoring of orchestrated attacks similar to those in the wild is a necessary first step in the object. The rest of the paper is organized as follows. Section II gives an introduction to burst high bandwidth attack. Section III gives a detailed describe of the controlled environment. Section IV presents simulation results of the test bed. Finally, conclusions and discusses the future work in Section V.

2 Bandwidth Attack Overview

The common denominator of all burst high bandwidth aggregate is the desire to cripple someone else's infrastructure by generating a traffic overload. Two

examples of this are bandwidth attacks and flash crowd events. Most organizations' Internet connections have between 1 and 155 megabits per second (Mbps) of bandwidth available. Attacks have been reported in the hundreds of Mbps and up, more than enough to saturate nearly any system on the Internet. This can have serious consequences for Web companies which rely on their online availability to do business. The relations between bandwidth attack and DoS attacks are illustrated in Figure 1.

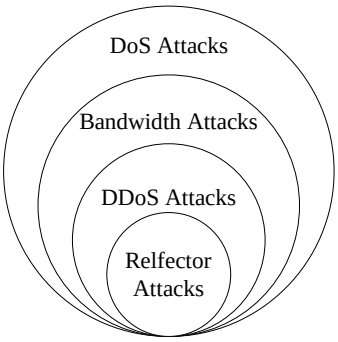

Fig 1: The relation of different types of attacks.

Flash crowds occur when a large number of users try to access the same server simultaneously. Apart from overloading at the server itself, the traffic from such flash crowds can overload the network links and thereby interfere with other, unrelated users on the Internet. For example, degraded Internet performance was experienced during a Victoria's Secret Webcast [1] and during the NASA Pathfinder Mission. A flash crowd event is similar to a DDoS attack from the traffic volume point of view. However, most of the source IP addresses of the flash crowd traffic have appeared in the network traffic monitoring point before, which has been justified in [2], videlicet it's predictable. Table 1 summarizes properties of flash crowd events and bandwidth attacks and their similarities and differences in broad terms.

Table 1: Comparative characteristics of flash crowd events vs. bandwidth attacks

Characteristic	Flash Crowd Events	Bandwidth Attacks
Traffic volume	both have a noticeable increase in terms of the number of requests. The length of peaks can be large or small depending on the episode	
Traffic type	mostly web	any
Number of clients and their distribution	follow population distribution among ISPs and networks.	across ISPs and networks does not follow population distribution
Cluster overlap	significant overlap	very small
Per-client request rates	lower during the event than usual	stable during the attack and significantly deviate from normal
Requested files	Zipf-like distribution	not Zipf-like
Predictability	mostly predictable	unpredictable

Bandwidth attacks are the result of several fundamental weaknesses of the Internet architecture:

1. Resource-sharing, the Internet is designed as an open public infrastructure to share information resources. This has two consequences. First, the potential victims, such as web servers, must connect to the Internet and be visible to the public in order to provide public service. The visibility is made via a globally routable IP address. Second, the Internet is based on packet-switching, unlike its counterpart, the public telecommunication network, which is based on circuit-switching. For circuit-switched networks, each service (e.g. a phone call) will be allocated a separate channel until the end of the service. A user's service will not be interfered by other users' behavior. In contrast, for packet-switched networks, users share all the resources and one user's service can be disturbed by other users' behavior. Bandwidth attacks take advantage of these two consequences: Attack packets will be delivered to the victim before knowing whether they are malicious or not. By occupying most of the shared resources, bandwidth attacks manage to disrupt the services for the legitimate users.

2. Authentication and traceability, the Internet is equipped with no authentication scheme, which leads to a serious problem, IP spoofing. Without an integrity check for each IP packet, attackers can spoof any field of an IP packet and inject it into the Internet. Moreover, the routers generally do not have packet tracing functions, for example, keeping all previous connection records. In practice, this cannot be done due to the huge amount of traffic that needs to be stored. Therefore, once an IP packet is received by the victim, there is no way to authenticate whether the packet actually comes from where it claims. By hiding their identities using IP spoofing, the attacker can launch bandwidth attacks

without being responsible for the damage.

3. Reliability of Infrastructure, Denial-of-service occurs when the attacker is able to consume the entire victim's resources, the Internet is a huge community, where many insecure systems exist. Unfortunately, the number of vulnerabilities reported each year is increasing according to CERT statistics, as shown in Figure 2. Hence, attackers can control a large number of insecure systems by exploiting their vulnerabilities. By launching bandwidth attacks from these controlled systems, the attack power is tremendously increased.

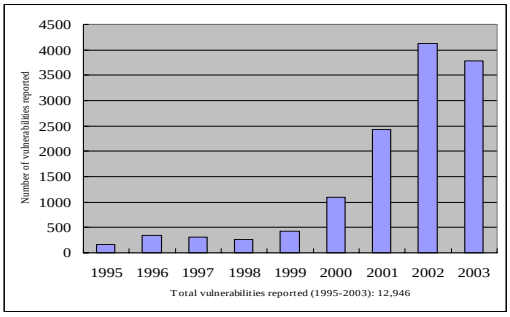

Fig 2: The number of vulnerabilities reported each year according to CERT

For this causation, many different types of bandwidth attacks exist see the table in Table 2. This classification uses three properties: protocol-type, distribution, and whether or not IP spoofing is involved. An adaptive protocol is one that adjusts its rate when packets get lost. TCP is an adaptive protocol. Examples of non adaptive protocols are UDP and ICMP.

Table 2: Bandwidth attack classification

Protocol Type		Not distributed	Distributed
Adaptive	TCP	stealth or spoofing flood	typical bandwidth attack, involve DDoS attack and distributed reflector denial of service
Unadaptive	UDP	flood and spoofing	
	ICMP		

The Distributed Denial of Service (DDoS) attack is a type of bandwidth attack, The attack power of a DDoS attack is based on the massive number attack sources instead of the vulnerabilities of one particular protocol. Various classification criteria are indicated in Figure 3 summarizes the taxonomy.

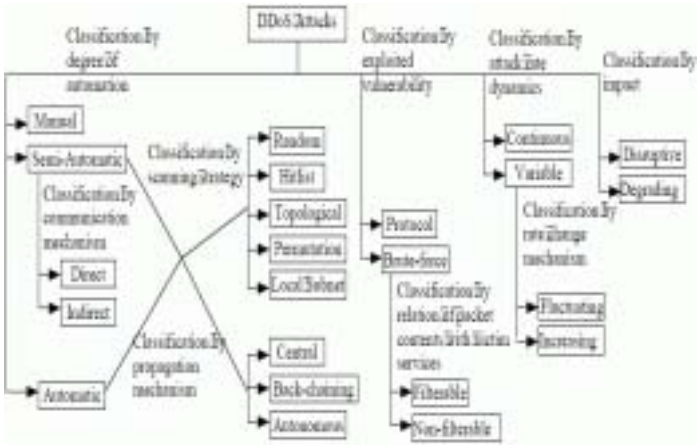

Fig 3: Taxonomy of distributed denial-of-service attack

3 Test Bed of Controlled Environment

The problem of burst high bandwidth (BHB) attacks suggests a need to have a controlled tentatively environment in which BHB attacks can be safely coordinated, and allowing attack detection and prevention schemes to be safely tested, without affecting operational networks. This environment should be provided with the following desirable characteristics:

1. Central control and monitoring of BHB attacks
2. Use of inexpensive components that are logically equivalent to their realistic counterparts with respect to experiments
3. Ability to tie in prevention schemes
4. Integration of the monitoring and prevention data

When analyzing computer network system, multiple approaches are available including closed-form analysis, test bed studies, and modeling and simulation. Closed form analysis is the most desirable of these since the resulting formulas and expressions can be quickly examined over multiple scenarios. Computer network system complexities typically rule out all but the simplest closed form analysis.

The second approach is modeling and simulation. The scenarios used in simulations and experiments reveal aspects of these mental models often including one or more of the following implicit assumptions [17]: Flows live for a long time and transfer a lot of data. Simple topologies, like a “dumbbell” topology with one congested link, are sufficient to study many traffic

properties. Flows on the congested link share a small range of round-trip times. Most data traffic across the link is one-way; reverse-path traffic is rarely congested. All of these modeling assumptions affect simulation and experimental results, and none of them are confirmed by measurement studies, therefore high fidelity models can't be easy to be verified and validated.

An alternative to analysis is the use of a test bed. There are various tools to launch BHB attacks [11-16]. Theoretically, no matter what attack tool is used, the basic feature of all types of BHB attacks is that attack packets coming from sources distributed all over the world has to be sent to an attacked site such that it denies services. Figure 4 presents a simplified timeline for the BHB attacks. The detect system of interest at this stage are T4-T5 [18], for this reason, that signs of BHB attacks can be detected by analyzing arrival data of a protected site is feasible.

Fig 4: A simplified timeline of BHB attack

The test bed setup consists of the following components: traffic generator, attack injection program, victim and sampling monitor. A experiment topology for controlled environment is given on Figure 5.

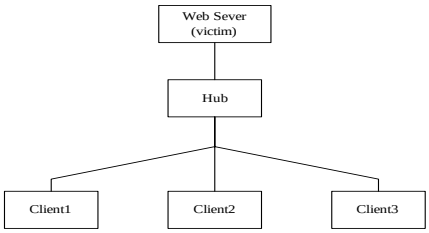

Fig 5: Experiment Network Topology

To generate testing traffic we integrated the annals payload of tcpdump wrapper, modeled payload and user-defined payload into the traffic generator system. Figure 6 shows the architecture of the generator.

The victim machine for this test bed was a web server running on a low-end machine that will be easier to break down.

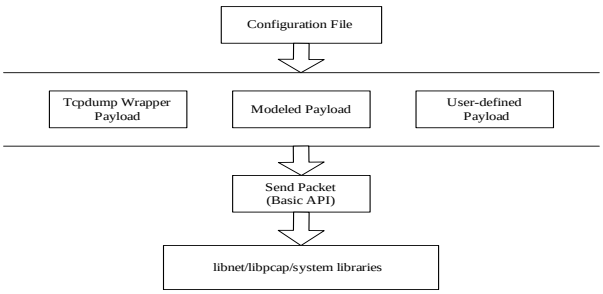

Fig 6: Traffic Generator architecture

A Java tool is used to generate BHB attack traffic, Figure 7 shows the architecture of the attack injection program.

Fig 7: attack injection program

Traffic monitor and sampling is classified common SNMP MIB(*Simple Network Management Protocol Management Information Base*) and the statistic way of on-line packet filtering, for instance NAI Sniffer and Agilent Internet Advisor. Owing to require the high frequency statistic of IP address and port, take into account controllable of the test bed, we adopted the statistic way of on-line packet filtering based on zero-copy architecture (Libppf sampling platform)[19]. The efficiency of samplings is compared in Figure 8.

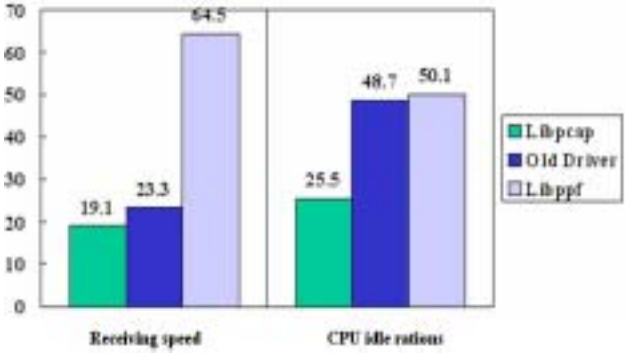

Fig 8: receiving speed & CPU idle ratios under three

platforms**4 A Simple Experiment with**

Controlled Environment

The test bed of proof-of-concept need to exhibit three characteristics:

1. Correct behavior in the absence of attack.
2. BHB attack traffic detection
3. Return to normal behavior when the attack decay

Figure 9 shows the rule of normal load with time varying. The type of BHB attack used is based upon HTTP, a great deal of packets(0-64 bytes) want to flood the web server, Figure 10-12 shows the real time

Fig 9: the rule of normal load with time varying

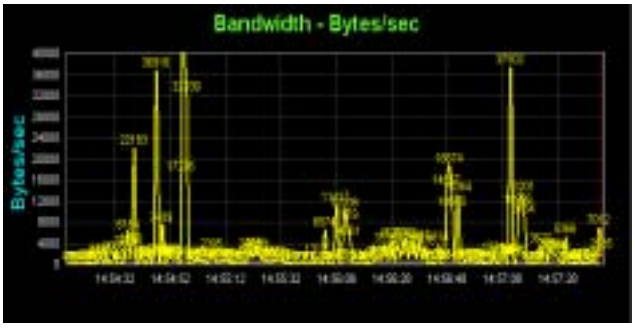

Fig10: the rule of BHB attack with time varying

parameter transformation of BHB attacks with time varying. The experiment is indeed successful in exhibiting the three desired experimental characteristics.

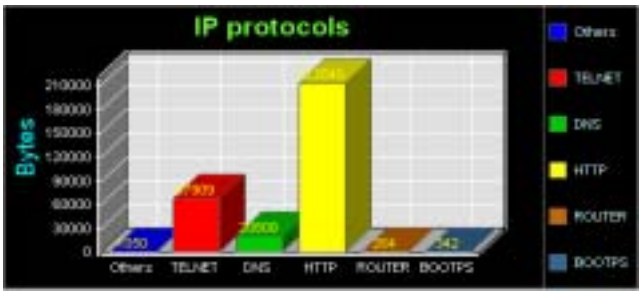

Fig11: the protocols distribution of BHB attack

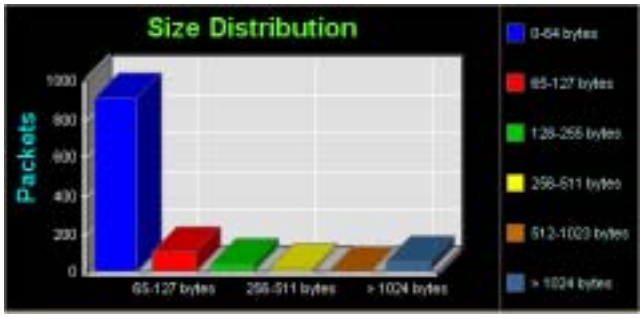

Fig12: the packets size distribution of BHB attack

5 Conclusions and Future Work

We have presented a controlled environment of BHB attacks simulation. This tested provides a neutral environment for collaboration where identify problems, and find solutions. On the other hand, it provides a venue for researchers to collaborate with identifiable pragmatic research topics and prototypical scenarios to advance the integration technology.

At present, research efforts are put into the following items:

1. specification and modeling of BHB attacks
2. effect of worm propagation on the network
3. how different types of BHB attacks will change the characteristics of the background traffic
4. generating high bandwidth traces through the structural model method for intrusion detection system evaluating

The controlled testbed is an essential step toward the successful development of new efficiency scheme for BHB attacks. The areas of research will be broadened as this controlled environment grows in the future.

References

[1] S. A. Paschos, F. N. Afrati. Common Security Attacks on a TCP/IP Environment, *In 3th WSEAS International Multiconference on Circuits, Systems, Communications and Computers,* Athens, Greece, July 4-9, 1999.

[2] Jaeyeon Jung, Balachander Krishnamurthy, and Michael Rabinovich. Flash crowds and denial of service attacks: Characterization and implications

for CDNs and web sites. *Proceeding of 11th Word Wide Web conference. Honolulu, Hawaii, USA.*

[3] S. Bellovin. The ICMP traceback message. Internet Draft, IETF, March 2000. draft-bellovin-itrace5.txt.

[4] Drew Dean, Matt Franklin, and Adam Stubblefield. An algebraic approach to ip traceback.

[5] In Network and Distributed System Security Symposium, NDSS '01, Feburary 2001.John Ioannidis and Steven M. Bellovin. Implementing pushback: Router-based defense against DDoS attacks. *In Proceedings of Network and Distributed System Security Symposium, Catamaran Resort Hotel San Diego, California. 6-8 February 2002. The Internet Society, February 2002.*

[6] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. *Controlling high bandwidth aggregates in the network*. Technical report, AT&T Center for Internet Research at ICSI (ACIRI) and AT&T Labs Research, February 2001.

[7] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. Practical network support for IP traceback. *In Proceedings of the 2000 ACM SIGCOMM Conference, August 2000.*

[8] Dawn X. Song and Adrian Perrig. Advanced and authenticated marking schemes for ip traceback. *In Proceedings of IEEE INFOCOM 2001, 2001*.

[9] S. Felix Wu, Lixia Zhang, Dan Massey, and Allison Mankin. Intension-Driven ICMP Trace-Back. Internet Draft, IETF, February 2001. draft-wu-itrace-intension-00.txt.

[10] Mirkovic, J., Martin, J., and Reiher, P. (2001). *A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms*. Los Angeles, CA, University of California Computer Science Department

[11] D. Dittrich, The DoS Project's 'Trinoo' Distributed Denial of Service Attack Tool, http://staff.washington.edu/dittrich/trinoo.analysis.

[12] D. Dittrich, The 'Tribe Flood Network' Distributed Denial of Service Attack Tool, http://staff.washington.edu/dittrich/tfn.analysis.txt.

[13] D. Dittrich, The 'Stacheldraht' Distributed Denial of Service Attack Tool, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt.

[14] CERT Coordination Center, CERT Advisory CA-1999-17 Denial-Of-Service Tools, http://www.cert.org/advisories/CA-1999-17.html.

[15] D. Dittrich, The 'Mstream' Distributed Denial of Service Attack Tool, http://staff.washington.edu/dittrich/misc/mstream.analysis.txt.

[16] S.Dietrich, N. Long and D. Dittrich, An Analysis of the 'Shaft' Distributed Denial of Service Tool,http://www.adelphi.edu/~spock/shaft_analysis.txt.

[17] S. Floyd and E. Kohler. *Internet Research Needs Better Models*. In Proceedings of HorNets-I, October 2002.

[18] J. B. D. Cabrera, L. Lewis, X. Qin, W. Lee, R. K. Prasanth, B. Ravichandran, and R. K. Mehra. Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables - A Feasibility Study. *In Proceedings of the Seventh IFIP/IEEE International Symposium on Integrated Network Management*, pages 609-622,Seattle, WA, May 2001.

[19] Xiaoqi L. *A Zero-copy Based High Performance Packets Acquisition and Dispatch Platform*. Dissertation for the Master Degree in Engineering. Harbin Institute of Technology. 2002.7

[20] Gaeil Ahn, Kiyoung Kim, Jongsoo Jang. "Effective traffic control scheme for protecting legitimate traffic from malicious traffic on internet". *In 2002 WSEAS International Conf. on Information Security, Hardware/Software Codesign, E-Commerce and Computer Networks*, Copacabana, Rio de Janeiro, Brazil, October 15-17, 2002