The Robust system for antivenin DDOS by Rioter Puddle Expertise

Amarjit Kaur
Department of Computer Science &Engineering,
Guru Nanak Dev University, Amritsar, India.
amark40@ymail.com

I INTRODUCTION

Secure communication has some anticipated security aspects such as confidentiality, authentication, message integrity and non repudiation. Besides, recently more people are aware that availability and access control are also urgent requirements of secure communication because of the dishonourable Denial of Service (DoS) attacks that render by the illegitimate users into a network, host, or other piece of network infrastructure to harm them, particularly it is done against the frequently visited websites of a number of high-profile companies or government websites. DDoS (Distributed Denial of Service) attack operates adequate puppet computers to create amount of data packets, the attacks become coordinated and come from multiple puppets at the same time thus are even devastating .A typical DDoS attack contains two stages, the first stage is to cooperation susceptible systems that are accessible in the Internet and install attack tools in these compromised systems. This is known as turning the computers into “zombies.” In the second stage, the attacker sends an attack command to the “zombies” through a secure channel to launch a bandwidth attack against the targeted victim(s).

1.1 OVERVIEW OF PUSHBACK

If we could unequivocally detect packets belonging to an attack and drop just those, the problem would be solved. However, routers cannot tell with total certainty whether a packet actually fits to a ‘good’ or a ‘bad’ flow; our goal will be to develop heuristics that try to identify most of the bad packets, while trying not to interfere with the good ones. Again, Mahajanet al. introduces the concept of Aggregate-based Congestion Control (ACC); in this context, an aggregate is defined as a subset of the traffic with an recognizable property. For example, “packets to destination D”, TCP SYN packets”, or even “IP packets with a bad checksum” are all potential descriptions of aggregates. The task is to identify aggregates responsible for congestion, and preferentially drop them at the routers.

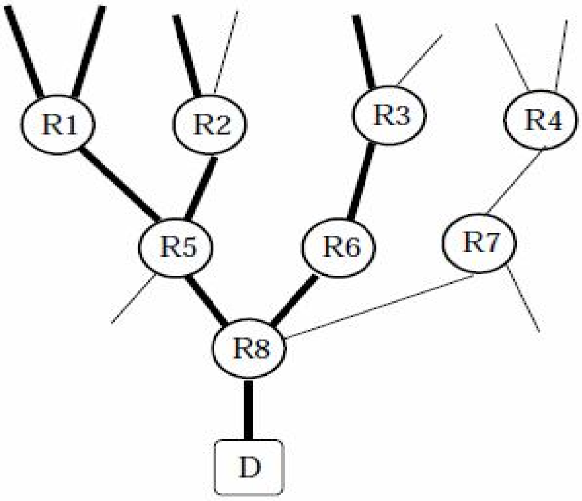


Figure 1. A DDoS attack in progress.

To illustrate Pushback, consider the network in Figure 1. The server □is under attack; the routers___ are the last few routers by which traffic spreads. The thick lines show links through which attack traffic is flowing; the thin lines show links with no bad traffic. Only the last link is actually congested, as the inner part of the network is adequately provisioned. In the absence of any special measures, hardly any non-attack traffic would be reaching the destination. Some non-attack traffic is flowing through the links between R2-R5, R3-R6 R5-R8, R6-R8, and from R8 to D, but most of it is dropped due to congestion in R8-D.

Through out this paper we shall be referring to 'good', 'bad', and poor' traffic and packets. Bad packets are those sent by the attackers. Bad traffic is categorized by an Poor traffic consists of packets that match the congestion signature, but are not really part of an attack; they are just unlucky enough to have the same destination, or some other properties that cause them to be recognized as belonging to the attack. Good traffic does not match the congestion signature, but shares links with the bad traffic and may thus suffer.

In the figure above, some of the traffic entering R4 is good (the part exiting R7 that is not going to R8), and some is poor, as it is going to D. There may be some good traffic entering R5 from the links above, and exiting from the lower left link, but depending on how jammed the links R1-R5and R2-R5 are, it may suffer. The other links have a mixture of bad and poor traffic. Now, no matter how smart filters R8 could employ, it cannot do anything to allow more good traffic originating from the left side of the graph to reach □. All it can do is preferentially drop traffic arriving from R5 andR6, hoping that more good traffic would flow in via R7. With Pushback, R8 sends messages to R5and R6 telling them to rate-limit traffic for. Even yet the links downstream from R5 and R6are not congested, when packets arrive at R8 they are going to be dropped anyway, so they may as well be dropped at R5 and R6. These two routers, in turn, propagate the request up to R1, R2, andR3, telling them to rate-limit the bad traffic, allowing some of the 'poor' traffic, and more of the good traffic, to flow through. In the rest of the paper, we shall describe router architecture and the corresponding algorithm that can implement this kind of defence, and present its implementation under FreeBSD.

1.2 ARCHITECTURE

Consider a typical router; Figure 2 gives the view of the routing mechanism from one output interface. There are several incoming links, and the routing subsystem is implicitly shown in the choice of the output border. A rate limiter is introduced before the output queue; some form of rate limiting or traffic shaping is already in place in many routers. For example, in the FreeBSD operating system [FBS], the IPFW firewall package also does traffic shaping. The simplest way to view the rate limiter is as a predicate that decides whether a packet is dropped or forwarded. In our architecture, dropped packets are sent to the pushback daemon, pushbackd. The daemon, in turn, periodically updates the parameters of the rate limiter, and also informs the upstream daemons to update theirs. It is interesting to note that the real Pushback daemon may not reside on the router itself, but rather on an external ancillary piece of equipment.

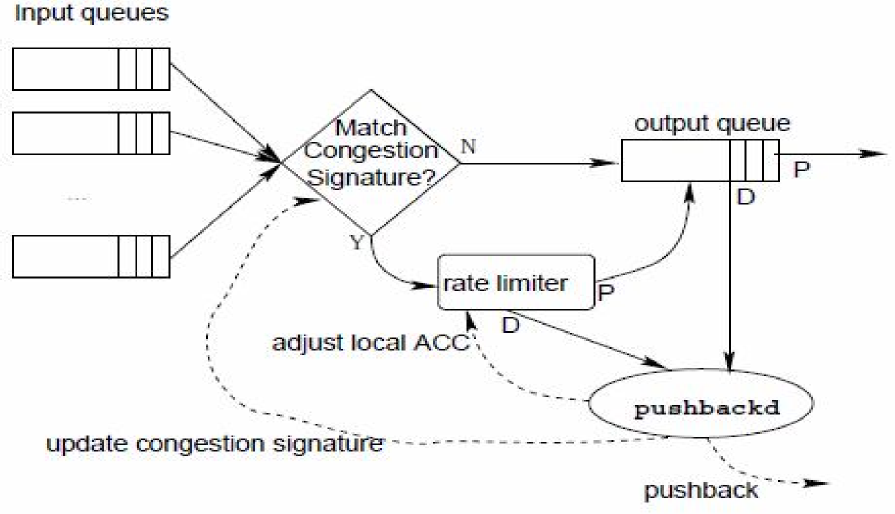
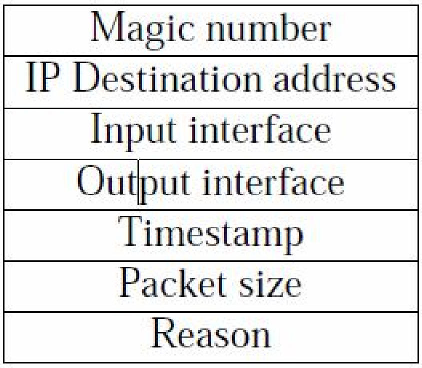


Figure 2. Partial view of a router.

The information sent to the Pushback spirit by the rate limiter is shown in Figure 3. Most of the fields have the obvious purpose. The magic number provides some protection against synchronization problems between the kernel and the user-level process. The timestamp is expressed in nanoseconds since the router was last booted, and its purpose, along with the packet size, is to allow the code3to estimate the bandwidth that would have been used up by the dropped packets. The 'reason' field indicates whether this was a tail-queue drop, a RED drop, and so on. Only packets dropped because of queue discipline restrictions are logged; packets dropped because, for example, they were not routable, or even because no buffer space could be allocated for them at the driver may not even reach this part of the code, so they are not informed at all. It is important to note that the design decision to separate the rate-limiting and packet-dropping functionality from the rest of the pushback mechanism has implications for the eventual deployment of such a mechanism in the Internet.



Magic number
IP Destination address
Input interface
Output interface
Timestamp
Packet size
Reason

Figure 3. **Dropped packet report**

Routers can be designed1 to report statistics about dropped packets, either to a process running on the router CPU, or a computer attached to the router using a local interface. All the intelligence, which would have to evolve rapidly as DDoS attacks change in nature, would reside in easy to replace, generic PCs, and scarce router resources do not have to be allocated to the Pushback task.

A. LITERATURE SURVEY

1. *A Review of DDOS Attack and its Countermeasures in TCP Based Networks, Akash Mittal, Prof. Ajit Kumar Shrivastava, Dr. Manish Manoria[2011]*

Efficiency and scalability are the key requirements in design of defence against DDoS Attacks. In this paper illustrate study of various DDOS attack techniques and prevention techniques [1]. All these method based on filtration mechanism and pattern matching based on the different normal or abnormal packet pattern. One great advantage of the development of DDoS attack and defence classifications is that effective communication and cooperation between researchers can be achieved so that additional weaknesses of the DDoS field can be identified DDoS attacks are not only a serious threat for wired networks but also for wireless infrastructures[2].On the basis of all these review, a Counter bloom filter Mechanism using the Independent component analysis has been proposed for the future work which will not only detect the DDOS traffic but also help in filtering that unwanted traffic.

2. *DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal [2006]*

In this paper, I have studied consider sophisticated attacks that are protocol-compliant, non-intrusive, and utilize legitimate application-layer requests to overwhelm system resources [8]. In this characterize application layer resource attacks as either request flooding, asymmetric, or repeated one-shot, on the basis of the application workload parameters that they exploit. To protect servers from these attacks, we propose a counter-mechanism that consists of asuspicion assignment mechanism and a DDoS-resilient scheduler, DDoS Shield.

3. *DDoS Mitigation via Regional Cleaning Centers, Sharad Agarwaly, Travis Dawson, Christos Tryfonasy[2004]*

Proposed to address the problem of Distributed Denial of Service (DDoS) attacks at the ISP level by introducing the concept of regional cleaning centers. Under this approach, traffic destined to a victim under a DoS (or DDoS) attack, is routed to a cleaning center for cleaning. After filtering out the malicious packets, the traffic is routed back to the original destination. It described the architecture of a cleaning center, identified its main components and explained the SLA requirements that need to be considered for this new service. It also presented a set of approaches to achieve traffic diversion and redirection which are essential for any implementation of a cleaning center. The availability of certain resources that each approach requires would determine its feasibility in certain environments. Finally, we showed results from a sample cleaning center in which it varied the approach used for both traffic diversion and redirection. The results indicate that cleaning centers can be a viable option for traffic conditioning, provided that its implications in the dynamics of traffic are part of a network-wide traffic engineering process.

4. *A Study on Recent Approaches in Handling DDoS Attacks, DebajyotiMukhopadhyay[2006]*

Present a study on the recent approaches in handling Distributed Denial of Service (DDoS) attacks. In this paper, it has presented four major approaches that are being considered by the experts in this field. Perhaps it will be a hard and impossible task to discuss each and every published work in this field and propose the best solution. That’s why it has kept the scope of the paper limited to just categorizing the existing solutions.

5. *Implementing Pushback: Router-Based Defense Against DDoS Attacks, John, Steven M. Bellovin[2001]*
Proposed Pushback, mechanism for defending against distributed denial-of-service (DDoS) attacks. It presented the implementation of a mechanism that treats Distributed Denial of Service attacks as a congestion-control problem, and acts by identifying and preferentially dropping traffic aggregates responsible for such congestion. The purpose of this work is twofold; show the practicality of such an approach, and explore ways to deploy it incrementally in an operational environment. It already knows from simulations that Pushback is a promising way of combating DDoS attacks and flash crowds. There are some aspects that are easy to simulate, but real code running on real machines allows us to explore the details of a real system. It also needed to see how much memory and computing power is needed to actually run Pushback, in the hope of influencing commercial router designers toward implementing Pushback in their code. A promising hybrid solution, which we plan to investigate over the next few months, is to use features such as the Committed Access Rate[5]in cisco routers to implement the rate-limiting, while sniffing traffic on both incoming and outgoing links of each router to detect congestion and dropped packets, even if the router itself cannot report those.

6. A HYBRID APPROACH TO COUNTER APPLICATION LAYER DDOS ATTACKS, S. Renuka Devi and P. Yogesh[2012]
Proposes a hybrid detection scheme based on the trust information and information theory based metrics. In this paper, an effective and efficient hybrid scheme against DDoS attacks based on trust value and information metric (entropy) is proposed. The proposed scheme provides double check point to detect the malicious flow from the normal flow. This approach not only counters the illegitimate flows but also avoids the flooding of the legitimate flows. Trust value is used to detect the legitimate user from the attackers at the first level. Then, based on the information metric of the current session, the sessions that are assumed to be suspicious are dropped. The legitimate flows are then scheduled by the scheduler based on the system workload the trust value of the client. Thus the legitimate clients get more priority in accessing the information and services.

7. A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms, JelenaMirkovic, Janice Martin and Peter Reiher[2004]
Proposes taxonomy of distributed denial-of service attacks and taxonomy of the defence mechanisms that strive to counter these attacks [3]. The attack taxonomy is illustrated using both known and potential attack mechanisms. Along with this classification we discuss important features of each attack category that in turn define the challenges involved in combating these threats[4].

III. GAPS IN CURRENT DEVELOPMENT MODELS

SYN flood attack
Any system providing TCP-based network services is potentially subject to this attack [5]. The attackers use half-open connections to cause the server exhaust its resource to keep the information describing all pending connections. The result would be system crash or system in operative [6].

TCP Reset Attack
TCP reset also utilize the characteristics of TCP protocol. By listen the TCP connections to the victim, the attacker sends a fake TCP RESET packet to the victim. Then it causes the victim to inadvertently terminate its TCP connection [7].

ICMP attack
Smurf attack sends forged ICMP echo request packets to IP broadcast addresses. These attacks lead large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, accordingly cause network congestion or outages [8]. ICMP datagram can also be used to start an attack via ping. Attackers use the ping Command to construct oversized ICMP datagram to launch the attack [9].

UDP storm attack
This kind of attack can not only impair the hosts. Services, but also congest or slow down the prevailing network [10]. When a connection is established between two UDP services, each of which produces a very huge number of packets, thus cause an attack [11].

DNS request attack
In this attack scenario, the attack sends a large number of UDP-based DNS requests to a name server using a spoofed source IP address [12]. Then the name server, acting as an intermediate party in the attack, responds by sending back to the spoofed IP address as the victim destination. Because of the amplification effect of DNS response, it can cause serious bandwidth attack [13].

ARP storm attack
During a DDoS attack, the ARP request volume can become very massive, and then the victim system can be negatively affected

Spam Attack
This type of attack is used for targeting the various mail services of corporate as well as public users.

DDoS attack through spam has increased and disturbed the mail services of various organizations [14]. Spam penetrates through all the filters to create DDoS attacks, which cause serious trouble to users and the data. But these mail services are frequent target of hackers and spammers [15].

IV. PROBLEM DEFINITION

Pushback is a mechanism for defending against distributed denial-of-service (DDoS) attacks. DDoS attacks are treated as a congestion-control problem, but because most such congestion is caused by malicious hosts not obeying traditional end-to-end congestion control, the problem must be handled by the routers. Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack. Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the router's resources be used to route legitimate traffic. Seeking limitations in existing work like pushback router based mechanism, I would be developing a counter mechanism for preventing DDOS attacks and also enhancing these existing models that are already the base for number of other researches but no real contribution has put to it. The Analysis will be done by using simulator.

V. REFERENCES

[1] Kihong Park; ***Scalable DDoS protection using route-based filtering***; DARPA Information Survivability Conference and Exposition, 2003. Proceedings Vol.2, 22-24 April 2003; Page(s):97.

[2] Hal Burch and Bill Cheswick. Tracing Anonymous Packets to Their Approximate Source.In *Usenix LISA*, December 2000.

[3] Steve M. Bellovin. ICMP Traceback Messages. Work in Progress, Internet Draft draftbellovin-itrace-00.txt, March 2000.

[4] Abraham Yaar, Adrian Perrig, Dawn Song; ***SIFF: a stateless Internet flow filter to mitigate DDoS flooding attacks***; Security and Privacy, 2004. Proceedings.2004 IEEE Symposium on 9-12 May 2004; pp.130 – 143.

[5] David D. Clark, Scott Shenker, and Lixia Zhang. Supporting Real-Time Applications in an Integrated Services Packet Network Architecture and Mechanism.In *ACM SIGCOMM*, 1992.

[6] Drew Dean, Matt Franklin, and A. Stubblefield. An algebraic approach to iptraceback, .In *Proceedings of NDSS '01*, February 2001.

[7] Basheer Al-Duwairi, ManimaranGovindarasu; ***Novel hybrid schemes employing packet marking and logging for IP traceback***; Parallel and Distributed Systems, IEEE Transactions on; Vol.17, No.5,May 2006; pp. 403-418.

[8] <http://cisco.com> viewed on 15 may 2010.

[9] S. M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Mosse, and T. Znati, "Proactive ServerRoaming for Mitigating Denial-of-Service Attacks," in Proceedings of the 1st InternationalConference on International Technology: Research and Education (ITRE'03), pp. 286-290, Aug.2003.

[10] A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoSattacks," in Proceedings of the IEEE symposium on Security and Privacy, pp. 93-109, May 2003.

[11] P. Feruson and D. Seine, "Network Ingress Filtering: Defeating Denial Of Service Attacks WhichEmploy IP Source Address Spoofing," RFC2827, May 2000.

[12] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent,and W. T. Strayer, "Single-Packet IP Traceback," IEEE/ACM Transactions on Networking, Vol.10, No. 6, pp. 721-734, Dec. 2002.

[13] J.Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense AgainstDDoSAttacks,"in Proceedings of the Network and Distributed System Security Symposium (NDSS'02),pp. 6-8, Feb. 2002.

[14] Yao Chen1, Shantanu Das, PulakDhar, Abdul-motaleb El Saddik, and AmiyaNayak, "Detectingand Preventing IP-Spoofed Distributed DoS Attacks," International Journal of Network Security,Vol.7, No.1, pp.70–81, Jul. 2008.

[15] Changlai Huang, Ming Li, Jianghu Yang, ChuanshanGao; ***A Real-Time Traceback Scheme For DDoS Attacks***; Wireless Communications, Networking and Mobile Computing, 2005. Proceedings; Vol.2, 23-26 Sept 2005; pp. 1175-1179.