Recent DDoS Incidents and Their Impact

Daljeet Kaur, Monika Sachdeva , Krishan Kumar

Abstract— In the present era Internet has changed the way of traditional essential services such as banking, transportation, power, health, and defence being operated. These operations are being replaced by cheaper, more efficient Internet-based applications. The explosive growth of the Internet and its increasingly critical role in supporting electronic commerce, transportation, and communications, have brought an equally explosive growth in attacks on Internet infrastructure and services. Some of the most difficult attacks to defend against are the Distributed Denial of Service (DDoS) attacks, in which an overwhelming flood of network packets is generated from many different sources, with the intent of preventing legitimate use of services. Denial-of-service attacks occur almost every day, and the frequency and the volume of these attacks are increasing day by day. In this paper, an overview on DDoS problem, major factors causing DDoS attacks are demonstrated and finally detail of most recent DDoS incidents on online organizations are outlined.

Index Terms— Availability, DDoS Incidents, Vulnerability, DoS, Bots, Zombies, bottleneck.

1 INTRODUCTION

With the increased availability of broadband access to the Internet and the lack of security associated with many university and home-user networks has come an increased proliferation of network-based attacks [1]. Compounding this problem is the increased reliance by the United States on the Internet as part of the critical infrastructure for electronic commerce and communications. Some of the most difficult network-based attacks are the Distributed Denial of Service (DDoS) attacks, in which an over-whelming flood of network packets are generated by many different sources, with the intent of preventing legitimate use of services. Typically, DDoS attacks are directed at one or more targets, such as end-users, web servers, entire networks or parts of networks, or networking infrastructure components (e.g., routers, communications links, load balancers, or firewalls). Distributed Denial of Service (DDoS) attacks have received much attention lately in the computing security community and in the industry at large. This can be attributed to the fact that the victims of these attacks have included well known web sites and electronic commerce companies. It is now estimated that the DDoS attacks in February 2000 on the CNN, Amazon, Buy.com, and Yahoo! Web sites caused millions of dollars in lost business [2]. Researchers and practitioners in the security community have long held that computer security has three primary objectives: confidentiality, integrity, and availability. A denial of service attack is fundamentally an attack on availability. The attacker seeks not to expose secrets or tamper with the victim's data, but to prevent the victim from effectively providing or using some service. DDoS attacks are a special class of denial of service attacks in which the attacker makes use of a large number of network-connected machines to carry out the attack.

The distributed denial of service problem is considered one of the most difficult security problems to solve. DDoS attacks are launched in a distributed and coordinated manner using automated agents on multiple machines. These agents are often difficult to locate as they may use spoofed source addresses. Many DDoS attack tools can be downloaded from well-known Internet hacker sites where new tools are being deployed at alarming rates. Accumulated experience by practitioners and researchers in dealing with denial of service (DoS) attacks has led to some consensus on the broad classification of these attacks. Attack classes include the following:

• Bandwidth consumption. These attacks consume all available bandwidth on one or more network links and thereby deny bandwidth to legitimate traffic. This may be accomplished in one of two ways. An attacker who has more available bandwidth than a victim's network can flood the victim's slower network connection. Alternatively, an attacker, even if using a slow network connection, can amplify the attack by using multiple sites to launch a distributed attack to flood the victim's network (see documentation on the Shaft tool [3]).

• System resource starvation. These attacks focus on consuming system resources such as CPU time, memory, and file-system usage quotas. By consuming these resources in an excessive manner, they are deprived for legitimate system and user needs.

• Exceptional condition exploitation. These attacks exploit design and programming flaws that result in the failure of an application, operating system, or hardware device to handle certain exceptional condi-

tions By inducing such conditions, the attack may slow down or disable the affected system. Some of the well-known attack techniques in this category involve sending malformed network packets to cause system crashes.

• Routing and Domain Name Service (DNS) manipulation. Routing-based DoS attacks involve malicious manipulation of routing table entries, causing network traffic to be improperly routed through the Internet. Attacks on DNS servers involve inducing these servers to cache bogus address information so that legitimate traffic is directed to the wrong Internet (IP) addresses. Either kind of attack may prevent the victim from properly sending or receiving network packets, or cause the victim to be flooded with packets misdirected to its network.

In principle, any of these denial of service attacks can be carried out in a distributed manner, as a DDoS attack, though distribution usually provides the most leverage in bandwidth consumption and system resource starvation attacks.

2 OVERVIEW OF DDOS ATTACKS

DDoS attacks involve breaking into hundreds or thousands of machines all over the Internet. Then the attacker installs DDoS software on them, allowing them to control all these burgled machines to launch coordinated attacks on victim sites. These attacks typically exhaust bandwidth, router processing capacity, or network stack resources, breaking network connectivity to the victims. The attacker runs a single command, which sends command packets to all the captured machines, instructing them to launch a particular attack (from a menu of different varieties of flooding attacks) against a specific victim. When the attacker decides to stop the attack, they send another single command. The controlled machines being used to mount the attacks send a stream of packets. For most of the attacks, these packets are directed at the victim machine. For one variant (called ``smurf'', named after the first circulated program to perform this attack) the packets are aimed at other networks, where they provoke multiple echoes all aimed at the victim. The operating systems and network protocols are developed without applying security engineering which results in providing hackers a lot of insecure machines on Internet. These insecure and unpatched machines are used by DDoS attackers as their army to launch attack. An attacker or hacker gradually implants attack programs on these insecure machines. Depending upon sophistication in logic of implanted programs these compromised machines are called Masters/Handlers or Zombies and are collectively called bots and the attack network is called botnet in hacker's community. Hackers send control instructions to masters, which in turn communicate it to zombies for launching attack.

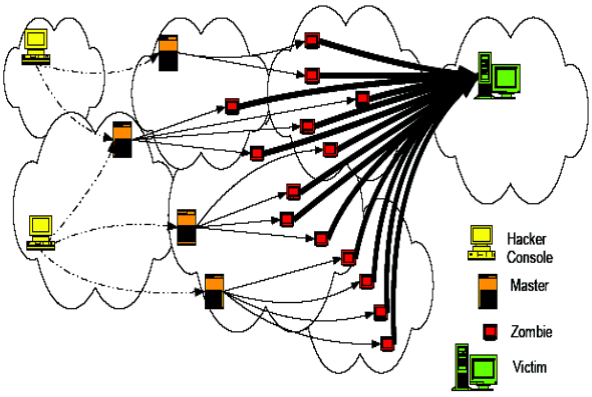

Fig. 1. Attack Modus Operandi.

The zombie machines under control of masters/handlers (running control mechanism) as shown in Fig 1 transmit attack packets, which converge at victim or its network to exhaust either its communica-tion or computational resources. Mirkovic et al. [4] have classified DDOS attacks into two broad catego-ries: flooding attacks and vulnerability attacks. Flood-ing DDoS attacks consume resources such as network bandwidth by overwhelming bottleneck link with a high volume of packets. Vulnerability attacks use the expected behaviour of protocols such as TCP and HTTP to the attacker's advantage. The computational resources of the server are tied up by seemingly legitimate requests of the attackers and thus prevent the server from processing transactions or requests from authorized users. Flooding DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors and buffers etc., the attackers bombard the scarce resource(s) by sheer flood of packets. In Figure 2 a flood of packets is shown, which congests the link between ISP's edge router and border router of victim domain

[5]. Attack packets keep coming as per distribution fixed by attacker, whereas legitimate clients cut short their packet sending rates as per flow control and congestion signals. A situation comes when whole of bottleneck bandwidth is seized by attack packets.
Thus, service is denied to legitimate users due to limited bottleneck bandwidth. However, resources of connecting network are not a problem in case of commercial servers as these are hosted by the ISPs, quite close to their backbone network with high bandwidth access links. But server resources such as processing capacity, buffer limit etc., are put under stress by flood of seemingly legitimate requests generated by DDoS attack zombies. Each request consume some CPU cycles. Once the total request rate is more than the service rate of server, the requests start getting buffered in the server, and after some time due to buffer over run, incoming requests are dropped. The congestion and flow control signals force legitimate clients to decrease their rate of sending requests, whereas attack packets keep coming. Finally, a stage comes when only attack traffic is reaching at the server.

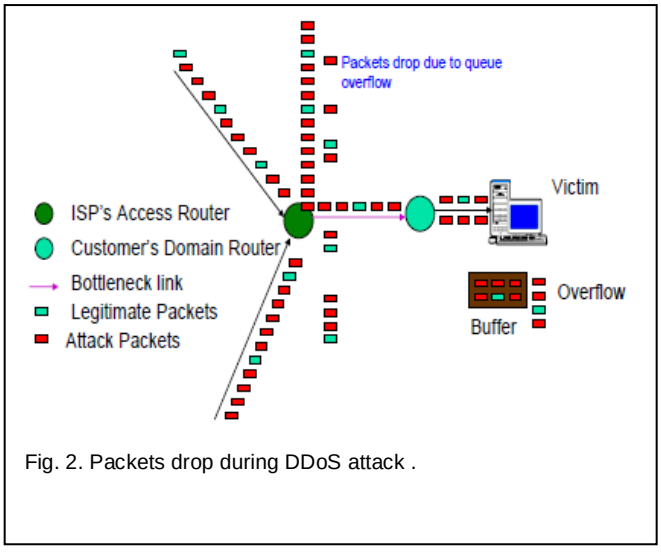

Fig. 2. Packets drop during DDoS attack .

Thus, service is denied to legitimate clients. Moreover Robinson stated that as attack strength grows by using multiple sources, the computational requirements of even filtering traffic of malicious flows become a burden at the target.
One of the major reasons that make the DDoS attacks wide spread and easy in the Internet is the availability of attacking tools and the powerfulness of these tools to generate attacking traffic [6]. As per [4], [7] various reasons that create opportunities for attackers to use attack tools easily and launch a successful attack are:
1) Internet security is highly interdependent: The susceptibility of DDoS attacks depends upon global internet security rather than the security of victim.
2) Internet resources are limited: Each Internet host has limited resources that can be consumed by a sufficient number of users.
3) Accountability is not enforced: With mechanisms like IP spoofing, the perpetrator can conceal his real identity and hence, real source of attack cannot be judged.
4) Control is distributed: Since Internet management is distributed and each network runs as per particular policies and regulations defined, it is almost impossible to deploy a certain global security mechanism and moreover due to privacy concerns it is sometimes nearly impossible to investigate the cross network behaviour.
5) Simple Core and Complex Edge: One of the design principles is that the Internet should keep the core networks simple and push any complexity into the end hosts [7], [8]. Hence, core routers don't make necessary authentication checks. The void of authentication checks at network level encourages undesired unauthorized attempts like IP spoofing, which is the major way of doing DDoS attack.
6) Multipath Routing: Multipath routing makes authentication difficult hence, it may encourage unauthorized activities. Intermediate router routes IP packet from source to destination & has no way of knowing that whether the IP packet it is forwarding is the legitimate packet or a spoofed one [7].

3 RECENT INCIDENTS

2010 should be viewed as the year distributed denial of service (DDoS) attacks became main stream, says Arbor Networks [9]. In its Sixth Annual Worldwide Infrastructure Security Report, released today, Arbor

Networks revealed that DDoS attack Size broke 100 Gbps for first time; up 1000% since 2005.

TABLE 1
RECENT DDOS ATTACKS

S.no	*Date*	*DDoS target/Incidents*	*Consequences/Description*
1.	March , 2012	South Korea and United states Websites	It is similar to those launched in 2009.
2.	January 1, 2012	Official Website of the office of the vice president of Russia	It caused the site to be down by more than 15 hours.
1.	November 5 to 12 , 2011	Asian Ecommerce Company	Flood of Traffic was launched and 250,000 Computers are infected with malware participated.
2.	November 10, 2011	Server	The traffic load has been immense with several thousands request per second.
3.	October 2011	Site of National Election Commission of South Korea	Attacks were launched during the morning when citizens would look up information .and attack leads to fewer turnouts.
4.	March 30, 2011	On Blogging Platform Live Journal	Experienced serious functionality problems for over 12 Hours and resumed on April 4 and 5, 2011
5.	December 8, 2010	Master Card, PayPal, Visa and Post Finance	Attack was launched in supportof WikiLeaks.ch and its founder. Attack lasts for more than 16 hours.
6.	November 30, 2010	Whistleblower site Wikileaks	Attack size was 10 Gbps. Caused the site unavailable to visitors. Attack was launched to prevent release of secret cables.
7.	November 28, 2010	whistleblower site Wikileaks	Attack size was 2-4 Gbps. Attack was launched just after it released confidential US diplomatic cables.
8.	November 12, 2010	Domain registrar Register.com	Impacted DNS, hosting and webmail clients. 24 hours of outage
9.	November 2, 2010	Burma's main Internet provider	Disrupted most network traffic in and out of the country for 2 days. Geopolitical motivated attack. Attack size was of 1.09 Gbps (average) & 14.58 Gbps (maximum) . Attack vectors were TCP Syn/rst 85%, flooding 15%.
10.	October 2010	MPAA & Indian tech firm Aiplex software	At least hundreds of 4chan users at once executed attack in Pro-piracy protest. Simple application Low Orbit Ion Cannon (LOIC) was used.
11.	September 2010	Fast growing botnet	Botnet's motive was to provide commercial service "IMDDOS" was discovered for launching DDoS attacks against any target.
12.	July and August, 2010	Irish Central Applications Office server	Attack was hit on four different occasions.
13.	June 2010	Broadband forum Whirlpool	Flooding DDoS attack. 9 hours of outage.
14.	June 2010	UK-based Jewish Chronicle	Website had to shut down its balanced coverage of the "Ashdod flotilla incident" immediately.
15.	May 2010	Botnet consisting of web servers was discovered	Rrather than individual PCs,servers were being used. An attacker named "Exeman" has infected around 400 web servers with a simple 40-line PHP script.
16.	May 2010	Vocus	Caused connectivity disruptions across multiple websites. 80 minutes of disruption.
17.	May 2010	Web24	Caused Connection issues for users of the Vocus network More than 12 hours of outage.
18.	April 2010	Optus	Sourced from China. 4 hours of outage.
19.	February 2010	Australian Parliament House website (www.aph.gov.au)	Attack was the part of protest by a group. 50 minutes of outage.

The year witnessed a sharp escalation in the scale and frequency of DDoS attack activity on the Internet with many high profile attacks launched against popu-lar Internet services and other well known targets. In addition to hitting the 100 Gbps attack barrier for the first time, application layer attacks hit an all-time high. "Nowadays, it is frighteningly easy for attackers to execute a DDoS attack. Botnet comprised of thousands of compromised PCs can be rented cheaply, and software capable of automating attacks can be acquired readily on the underground market," writes Ram Mohan, EVP and CTO at Afilias and a regular Security Week contributor. "A distributed denial of service attack is every business's worst nightmare. One minute, everything is ticking along as normal. The next, your infrastructure is hit by a tsunami of spurious traffic from across the Internet. Legitimate users find themselves locked out, your ability to do business online grinds to a halt, and there's not a great deal you can do about it – unless you prepare ahead of time."

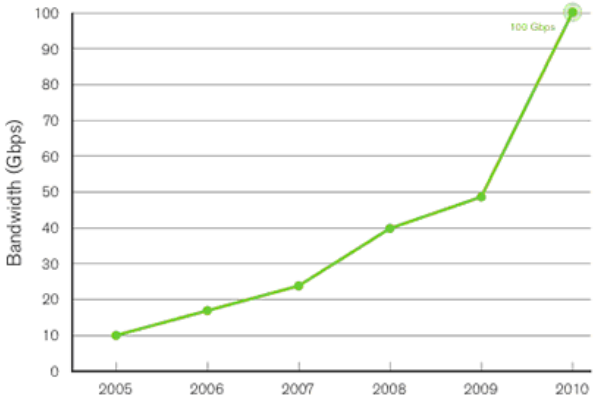

Fig. 3. Largest Single DDoS Attack Observed per Survey .

Arbor Networks[9] suggests that Botnet-driven DDoS attacks are likely to continue as a low cost, high-profile form of cyber-protest in 2011 and beyond. Major incidents in 2010 included DDoS attacks associated with the territorial disputes between China and Japan, the ongoing political turmoil in Burma and Sri Lanka and the WikiLeaks affair. The need to protect availability has finally made it onto the radar screen of enterprise IT consulting firms worldwide, and DDoS defense has consequently reached the status of a CXO-level issue globally. The attack has been successful in being a nuisance, said Jose Nazario, a botnet expert and senior security engineer for Arbor Networks. The attacker has chosen to flood only top level domains with traffic, temporarily shutting them down, but the agencies behind them can continue day-to-day operations, he said. "The types of attacks being thrown here are very common and have been common for many, many years," Nazario said. "This attack is requesting [Web] pages and content that is easily obtainable. The attacks are trivial to detect and trivial to thwart."
The DDoS attacks were launched last weekend, taking down several U.S. government sites, including the Federal Trade Commission and the U.S. Department of Transportation (DOT) as well as some South Korean government sites. Other high profile websites were targeted, including the New York Stock Exchange (NYSE), the Nasdaq electronic exchange and the Washington Post. The attacks continued Thursday, with some South Korean-based websites being inundated with traffic, including the website hosting the homepage of the U.S. Forces Korea.
Researchers from the U.S. Computer Emergency Readiness Team (US-CERT) and the Korea Internet Security Center are analyzing the code used to conduct the attacks and the traffic packets used to overload the websites. In addition, law enforcement, independent security researchers, ISPs and research teams at some security vendors are sharing research that could help trace the attacks back to the source, Nazario said.
The attacks consist of different types of traffic including standard HTTP request flooding, user datagram protocol (UDP) and transmission control protocol (TCP) packets. Most of the traffic is lightweight, easy to generate and send long distances. The attacks are not statically configured, Nazario said. Investigators have determined there is a command and control server directing the botnet. Early in the analysis, security researchers thought there was no command and control server. But the attacker is altering his tactics after the DDoS attacks have been mitigated. New targets and new commands are sent out periodically, Nazario said.
The attacker used a variant of the 2004 Mydoom worm to infect about 50,000 computers. Researchers say 90% of the victim machines are in South Korea. A small number of computers were infected in the U.S. It appears that the spam messages used to infect the machines were in Korean language and directed users to Korean language attack websites. According to a survey conducted by CSI in 2007, DDoS attacks were found to be one of the major reasons for financial losses [10] as depicted in Fig. 4, incurred almost $2,888,600 which is remarkable high sum of financials.

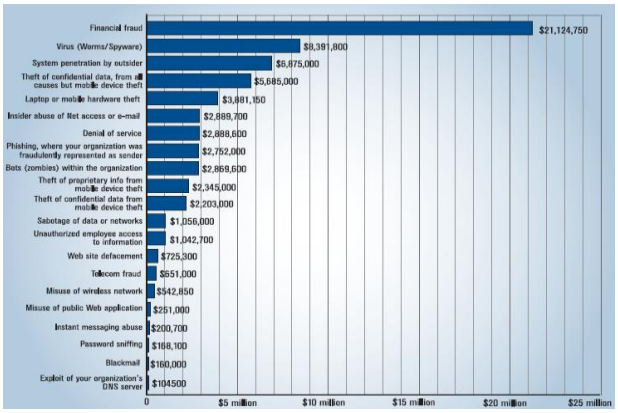

Fig 4. Financial losses incurred due to various attack incidents in 2007

A survey of CSI conducted in 2007 also showed that DDoS attacks were among major reasons of economical losses. While most companies are often reluctant to publicize the attacks they incur [11]. The increased numbers of DDoS attacks in volume and frequency have led to development of numerous defense mechanisms. Still, the growing number of attacks and their financial implications highlighted the need of a comprehensive solution. Distributed defense is the only workable solution to combat DDoS attacks [12]. There is a need of better ways to elicit the details of these attacks, only then a comprehensive distributed defense against DDoS attacks can be devised.

4 Conclusion

There is an alarming increase in the number of DDoS attack inci-dents. People should protect the network from attacks and mis-conduct. In this paper, we have explained DoS and DDoS prob-lem. Financial loss incurred due to DDoS attacks is also explored. DDOS can be prevented to a certain extend, if hosts and networks are secure. So each server owners and network owner should implement security measures on their network, if they want to fight against DDOS.

Acknowledgment

We would like to express our gratitude to all those who gave us the possibility to complete this paper work. We are extremely thankful to all the colleagues and faculty members for their constructive criticism and guidelines.

References

[1] D. Moore, G. Voelker and S. Savage, "Inferring Internet Denial of service Activity" Published in proceedings of the 2001 USENIX Security Symposium. The full paper in PDF is located at http://www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf,

[2] Cyber crime bleeds U.S. corporations, survey shows; finacial losses for attacks climb for 3rd year in a row, April 7, 2002. http://www.gocsi.com/prelea/000321.html

[3] S. Dietrich, N. Long, and D.Dittrich, "Analyzing Distributed Denial of Service Tools: The Shaft Case", Proceedings of the LISA XIV, December 3-8, 2000, New Orleans, LA.

[4] J. Mirkovic and P. Reiher "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," Computer Journal of ACM SIGCOMM, vol. 34, no. 2, pp. 39-53, 2004.

[5] K. Kumar, R. Joshi, and K.Singh, "An Integrated Approach for Defending Against Distributed Denial of Service Attacks," http://www.cs. Iitm .eret.in/~iriss06/paper.html, 2002.

[6] B.Gupta, R. Joshi, and M. Misra, "Distributed Denial of Service Prevention Techniques," International Journal of Computer and Electrical Engineering, Vol. 2, no. 2, pp. 268-276, April, 2010.

[7] [Peng,T., Leckie, C. and Ramamohanarao,K. "Survey of network based defense mechanisms countering the DoS and DDoS problems," Computer Journal of ACM Computing Surveys, vol. 39, no. 1, pp. 123-128, Apr. 2007.

[8] J. Mirkovic, "D-WARD: source end defense against distributed denial of service attacks," Ph.D. thesis, University of California, 2003.

[9] DDoS Attacks Exceed 100 Gbps, Attack Surface Continues to Expand By Mike Lennon on February 01, 2011 available at http://www.securityweek.com/ddos-attacks-exceed-100-gbps-attack-surface-continues-expand

[10] (2007) gocsi.com, "The 12th annual computer crime and security survey," [Online]. Available: http://www.sis.pitt.edu/~jjoshi/courses/ IS2150/Fall09/CSIFBI2007.pdf.

[11] (2009) Level3.com, "Managed DDoS Protection," [Online]. Available: http://www.level3.com/downloads/Managed_ DDoS_ Protection_whitepaper.pdf.

[12] M.Sachdeva, G. Singh, K. Kumar, and K.Singh, "A comprehensive survey of distributed defense techniques against DDoS attacks," International Journal of Computer Science and Network Security, vol. 9,no. 12, pp. 7-15, Dec. 2009.