DDoS Incidents and their Impact: A Review

Monika Sachdeva[1], Gurvinder Singh[2], Krishan Kumar[1], and Kuldip Singh[3]
[1]Department of Computer Science and Engineering, SBS College of Engineering and Technology, India
[2]Department of Computer Science and Engineering, Guru Nanak Dev University, India
[3]Department of Electronics and Computer Engineering, Indian Institute of Technology, India

Abstract: *The phenomenal growth and success of Internet has changed the way traditional essential services such as banking, transportation, medicine, education and defence are operated. Now they are being progressively replaced by cheaper and more efficient Internet-based applications. In present era, the world is highly dependent on the Internet and it is considered as main infrastructure of the global information society. Therefore, the availability of Internet is very critical for the socio-economic growth of the society. However, the inherent vulnerabilities of the Internet architecture provide opportunities for a lot of attacks on its infrastructure and services. Distributed denial-of-service attack is one such kind of attack, which poses an immense threat to the availability of the Internet. One of the biggest challenges before researchers is to find details of these attacks because to avoid defamation most of the commercial sites do not even reveal that they were attacked. In this paper, an overview of distributed denial-of-service problem and Inherent vulnerabilities in the Internet architecture are provided. Real distributed denial-of-service incidents with their financial impact are critically analyzed and finally need for a comprehensive distributed denial-of-service solution is highlighted.*

Keywords: *Availability, botnet, DoS, DDoS, incident, vulnerability.*

Received April 18, 2008; accepted June 8, 2008

1. Introduction

The "availability" means that the information, the computing systems, and the security controls are all accessible and operable in committed state at some random point of time [40]. Threat to the Internet availability is a big issue which is hampering growth and survival of e-business and other Internet based applications. The Internet like any other product is also prone to failures. Internet failures can be accidental or intentional. The Internet design concentrates mainly on providing functionality though a little attention has been given on designing strategies for controlling accidental failures. On the other hand, intentional attacks by malicious users/hackers/crackers have no answer in the original Internet design. A Denial of Service (DoS) is such an intentional attempt by malicious users/attackers to completely disrupt or degrade (compromise) availability of service/resource to legitimate/authorized users [7]. Some well-known DoS attacks are SYN Flood, teardrop, smurf, ping of death, land, finger bomb, black holes, octopus, snork, ARP Cache poisoning and the misdirection. DoS attacks exploit weaknesses in internet protocols, applications, operating systems, and protocol implementation in operating systems.

Distributed Denial of Service (DDoS) attacks degrade or completely disrupt services to legitimate users by expending communication and/or computational resources of the target. Mirkovic *et al.* [29] and Chang *et al.* [4] described DDoS attacks as amplified form of DoS attacks, where attackers direct hundreds or even thousands of compromised hosts called zombies against a single target. These zombie hosts are unwittingly recruited from the millions of unprotected computers accessing the Internet through high-bandwidth and always available connections.

There are varieties of DDoS attacks as classified in [15, 29]. However, the most common form of DDoS attacks is a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination. As per Peng *et al.* [36], defending against these attacks is challenging for mainly two reasons. First, the number of zombies involved in a DDoS attack is very large and deployment of these zombies spans large geographical areas. The volume of traffic sent by a single zombie might be small, but the volume of aggregated traffic arriving at the victim host is overwhelming. Second, zombies usually spoof their IP addresses under the control of attacker, which makes it very difficult to trace the attack traffic back even to zombies. According to the Internet architecture working group [21], the percentage of spoofed attacks is declining, but the sheer volume and distributed nature of DDoS attack traffic still thwart design of an effective defense.

In section 2, DDoS attack modus operandi and how DDoS denies services to legitimate clients are discussed. Section 3 explains why technically DDoS attacks are possible on the Internet. DDoS defense

challenges and principles are briefed in section 4. Section 5 details various DDoS incidents with financial impact in chronological order. Section 6 outlines need for effective DDoS solution. Finally section 7 concludes the paper.

2. DDOS Overview

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. The zombie machines under control of masters/handlers (running control mechanism) as shown in Figure 1 transmit attack packets, which converge at victim or its network to exhaust either its communication or computational resources.

Mirkovic *et al*. [29] have classified DDOS attacks into two broad categories: flooding attacks and vulnerability attacks. Flooding 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.

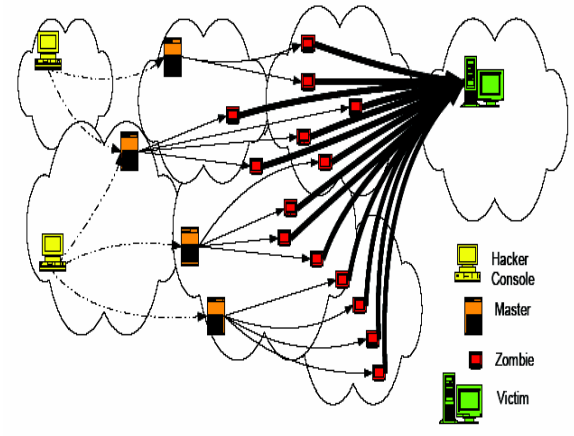

Figure 1. Attack modus operandi.

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 [26]. 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.

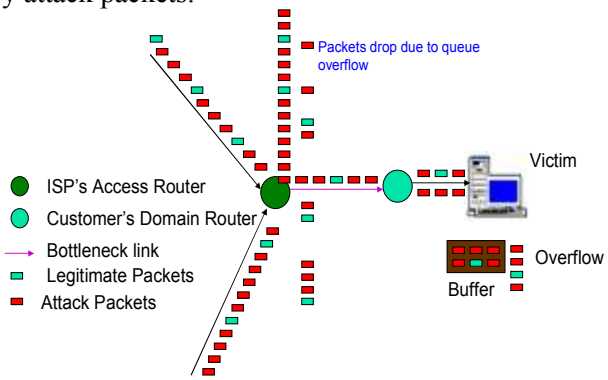

Figure 2. Packets drop under DDoS attack.

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, as shown in Figure 2, 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. Thus, service is denied to legitimate clients. Moreover Robinson *et al.* [37] 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.

3. Vulnerabilities

The Internet was designed with functionality, not security, in mind [39]. So its architecture has some inherent weaknesses and bugs called vulnerabilities, which result in successful origin and execution of DDoS attacks. The protection of Internet from DDoS attacks, i.e., DDoS defense has to compromise with these Internet design constraints and still provide a solution, which can offer Internet services to legitimate clients as per QoS requirements. Mirkovic *et al.* [29] and Chang *et al.* [4] have highlighted some of these vulnerabilities:

- Connectivity and 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 networks, which are based on circuit-switching. For circuit-switched networks, each service (e.g., a phone call) is allocated a separate channel until the end of the service. A user's service is not being interfered by other users' behaviour. In contrast, for packet-switched networks, users share all the resources and one user's service can be disturbed by other users' behaviour. Flooding attacks take advantage of these features. First, attack packets are delivered to the victim before knowing whether they are malicious or not. Second, by occupying most of the shared resources, flooding attacks manage to disrupt the services for the legitimate users.
- Authentication, integrity and traceability: the Internet is equipped with no inbuilt authentication scheme, which leads to a serious problem, called IP spoofing. IP spoofing [22] refers to creating an IP packet containing fake information. IP source address spoofing occurs when one IP packet is generated without using the source IP address that is assigned to the computer system. 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. They only receive and forward the packets. 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 and what it contains. By hiding their identities and integrity using IP spoofing, the attacker can launch flooding attacks without being responsible for the damage.
- Internet security is highly interdependent: 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 [8]. We can secure our system but we cannot force others to do so. Hence an attacker can control a large number of insecure systems by exploiting their vulnerabilities. By launching flooding attacks from these controlled systems, the attack power is tremendously increased.
- Intelligence and resources asymmetry: most of Intelligence needed for service guarantees is located in end hosts. But high bandwidth links and routers are in the intermediate network. So attackers can exploit the abundant resources of intermediate unwitting network to send malicious packets to explode processing, memory and bandwidth capacity of victims.
- Lack of centralized control on Internet: the Internet is an aggregation of numerous networks, connected with each other to provide global access to end users. Each network is run according to local policies defined by its owners. There is no central authority or management hierarchy, which has overall control over all networks on the Internet. Consequently, the most obvious disadvantage to DDoS defenders is that no security policy can expect its global deployment due to privacy and other commercial concerns. Moreover, different modules of distributed security systems cannot cross their administrative boundaries on the Internet without explicit cooperation.

4. DDoS Defens

The main aim of a DDoS defense system is to relieve victim's resources from high volume of counterfeit packets sent by attackers from distributed locations, so that these resources could be used to serve legitimate users. There are four approaches to combat with DDoS menace as proposed by Douligeris *et al.* [15]: Prevention, Detection and Characterization, Traceback, and Tolerance and Mitigation. Attack prevention aims to fix security holes, such as insecure protocols, weak authentication schemes and vulnerable computer systems, which can be used as stepping stones to launch a DoS attack. This approach aims to improve the global security level and is the best solution to DoS attacks in theory. Attack detection aims to detect DDoS attacks in the process of an attack and characterization helps to discriminate attack traffic from legitimate traffic. Traceback aims to locate the attack sources regardless of the spoofed source IP addresses in either process of attack (active) or after the attack (passive). Tolerance and mitigation aims to eliminate or curtail the effects of an attack and try to maximize the Quality of Services (QoS) under attack. Carl *et al.* [3], Douligeris *et al.* [15], and Mirkovic *et al.* [29] have reviewed a lot of research schemes based on these approaches but still no comprehensive solution to tackle DDoS attacks exist. One of the main reasons behind it is lack of comprehensive knowledge about DDoS incidents. Moreover the design and implementation of a comprehensive solution which can defend Internet from variety of DDoS attacks is hindered by following challenges:

- Large number of unwitting participants [29, 34].
- No common characteristics of DDoS streams [31].
- Use of legitimate traffic models by attackers [36].
- No administrative domain cooperation [32, 38].
- Automated DDoS attack tools [9, 11, 12, 13, 14].

- Hidden identity of participants because of source address spoofing [22].
- Persistent security holes on the Internet [20].
- Lack of attack information [29].
- Lack of standardized evaluation and testing approaches [3, 30].

In order to build a comprehensive DDoS defense solution in light of these challenges, Robinson *et al.* [37] recommended following DDoS defense principles:

- As DDoS is a distributed attack and because of high volume and rate of attack packets distributed instead of centralized defense is the first principle of DDoS defense.
- High Normal Packet Survival Ratio (NPSR) (ratio of number of normal packets received to total number of packets reaching at the server), i.e., less collateral damage is the prime requirement for a DDoS defense.
- A DDoS defense method should provide secure communication for control messages in terms of confidentiality, authentication of sources, integrity and freshness of exchanged messages between defense nodes.
- A partially and incrementally deployable defense model is successful as there is no centralized control for Autonomous Systems (AS) in Internet.
- A defense system must take into account future compatibility issues such as interfacing with other systems and negotiating different defense policies.

5. DDoS Incidents

The attacker/malicious users waste their energy and effort to create attack network called botnet, which comprises of weakly secured machines to launch such attacks. The main motives behind DDoS attacks are either of criminal**,** commercial or ideological nature. Broadly speaking, there are usually four types of attackers:

- Criminals who blackmail their victims and demand high ransom payments.
- Competitors who aim to damage their rivals business and reputation.
- Terrorists who carry out ideologically motivated attacks.
- Script kiddies who are testing their abilities or for publicity.

Extremely sophisticated, user friendly and powerful DDoS toolkits [2, 9, 11, 12, 13, 14] are available to potential attackers increasing the opportunity of launching of these attacks. The DDoS attack tools are so simple to use that nothing more than the whim of a 13-year old hacker is required to knock any user site, or server off the Internet. Moreover, DDoS attacking programs have very simple logic structures and small memory sizes making them relatively easy to implement and hide. Therefore, DDoS has emerged as the weapon of choice for disruption on the Internet.

Various DDoS attacks against high-profile websites such as Yahoo, CNN Amazon and E Trade in early 2000, series of attacks on grc.com in May, 2001 [18] and mydoom virus attack on SCO website in Feb. 2003 demonstrate how devastating DDoS attacks are and how defenceless the Internet is under such attacks. The services of these websites were unavailable for hours or even days as a result of these attacks. Therefore, the already grown dependence on the Internet makes the impact of successful DDoS attacks, financial and otherwise increasing painful for service providers, enterprises, and government agencies. Beginning from simple DoS security incidents, some of other well known packet flooding attacks and their impact are given below.

Real DoS incidents in the Internet between the years 1989 and 1995 were investigated in [24]. The three most typical effects were the following: 51% of these incidents filled a disk, 33% of the incidents degraded network service, and 26% of the incidents deleted some critical files. A single incident was able to cause several types of damages at the same time (the sum of percentages is more than 100%).

The first reported large-scale DDoS attack occurred in August, 1999, against a university [17]. This attack shut down the victim's network for more than two days. In February 7, 2000, several Web sites were attacked, which caused them to go offline for several hours [17]. As per Moore *et al.* [33] in some cases these DDoS attacks were able to produce about 1 Gbit/s of attack traffic against a single victim .

The backscatter analysis was used to assess the number, duration, and focus of DoS attacks in the Internet [34]. Backscatter is called the unsolicited response traffic which the victim sends in response to attack packets with spoofed IP source addresses. The results indicate more than 12,000 attacks against more than 5,000 distinct victims during the 3-week period examined in February, 2001. The Coordination Center of the Computer Emergency Response Team (CERT) even was attacked in May, 2001. This DDoS attack caused its affected web site to be available only intermittently for more than two days [25].

The Domain Name System (DNS) is a continuous target for DoS attacks. In October, 2002, all root name servers experienced an exceptionally intensive DoS attack. Some DNS requests were not able to reach a root name server due to congestion caused by the DoS attack. As per Gonsalves [19], another major DoS attack was launched on June 15, 2004 against name servers on Akamai's Content Distribution Network (CDN), which blocked nearly all access to many sites for more than two hours.

The affected sites included Apple computer, Google, Microsoft, and Yahoo. These companies have

outsourced their DNS service to Akamai to enhance service performance.

In UK online bookmaking, betting, and gambling sites have been extorted with DoS attacks during 2004 by unidentified attackers [28]. The Internet-based business service of Al Jazeera was brought down due to a DoS attack in January, 2005 [23]. Al Jazeera provides many Arabic-language news services. The text-to-speech translation application running in the Sun Microsystem's Grid computing system was disabled with a DoS attack in March, 2006 [16]. This attack was carried out during the opening day of this service.

Moore *et al.* [33], have established presence of roughly 2000-3000 active DoS attacks per week using updated backscatter analysis in their work. The study of attacks over a three-year period revealed 68,700 attack on over 34,700 distinct Internet hosts belonging to more than 5,300 distinct organizations. The Table 1 lists some of the recent DDoS attacks incidents.

Table 1. Recent DDoS incidents on important web sites.

Site Name	Date of Attack	Details
WordPress.com	February 19, 2008	6 Gigabits of incoming traffic 246 attacks 15 minutes of outage
Onlinecasino.com	February 18, 2008	170 attacks reported
Casinoeuro.com	February 15, 2008	177Mbps of incoming traffic 149 attacks 15 minutes of outage
Sciencetology.org	January 19, 2008	220Mbps of incoming traffic 30 minutes of outage
DSL.com	Dec.,2007	48MBps of malicious data, although traffic was less, attack was more of open connection request from an ever-growing list of IPs
Castlecops.com	July,2007	1 GBps of traffic 2 days of outage loss of more than $1,60,000.
Estonian sites pol.ee www.riigikogu.ee www.riik.ee www.peaminister.ee www.valitsus.ee m53.envir.ee www.sm.ee www.agri.ee 4 213.184.50.6/32 www.fin.ee 1 62.65.192.24/32	May, 2007	Ranging from 10-95Mbps 128 attacks 1-10 hours of outage

As proof of these disturbing trends, 2003 to 2006 FBI/CSI surveys [10, 20] concluded that DoS/DDoS attacks are one of the major causes of financial losses as depicted in Figure 3 below:

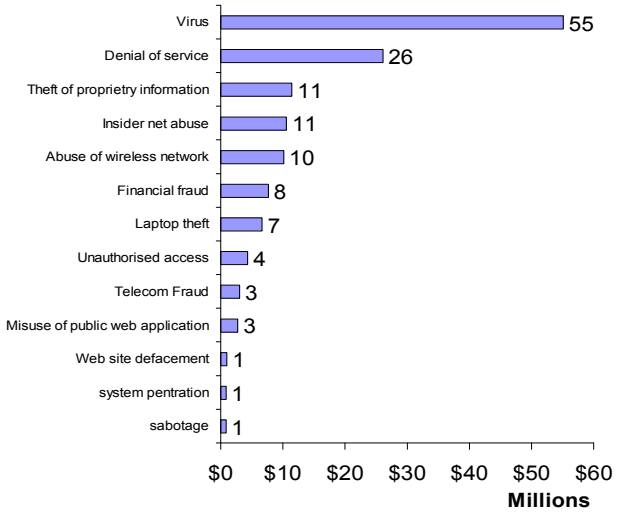

Figure 3. Financial losses incurred due to attack incidents.

6. Discussion

The traditional security technologies such as firewalls [6, 27, 35] Intrusion Detection Systems (IDSs) [1] and access control lists in routers are unable to defend networks from these attacks. The stumbling barrier against these attacks is that it is almost impossible to differentiate between genuine and attack packets. Since the potency of flooding DDoS attacks does not depend upon exploitation of software bugs or protocol vulnerabilities, it only depends on the volume of attack traffic. Consequently, flooding DDoS packets do not need to be malformed, such as invalid fragmentation field or a malicious packet payload. As a result, the flooding DDoS traffic looks very similar to legitimate traffic [29]. Also IP spoofing [22] and stateless routing reduces the chances of attacker being caught. Moreover, flooding DDoS attacks are very dynamic to elude existing defense systems [3, 29]. Therefore, it has become a real challenge to defend against these attacks. The seriousness of DDoS problem and growing sophistication of attackers have led to development of numerous defense mechanisms [5, 29]. But still, the growing number of DDoS attacks and their financial implications press the need of a comprehensive solution. Moreover, as attackers share their attack codes similarly to fight against these attacks, Internet community needs to devise better ways to accumulate details of attack. Only then a comprehensive solution against DDoS attacks can be devised.

7. Conclusion

The major contributions of this paper are:

- It gives a deep insight into DDoS problem and its origin.

- DDoS defense challenges and requirements are put in one place.
- Chronological information about DDoS incidents is provided.
- Last one year scenario of DDoS incidents on various sites is explored.
- The need for accumulation of DDoS attack information using systemized approaches is highlighted.

References

[1] Bai Y. and Kobayash H., "Intrusion Detection Systems: Technology and Development," *in Proceedings of the 17th International Conference on Advanced Information Networking and Applications*, USA, pp. 710-715, 2003.

[2] Barlow J., "TFN2K: An Analysis," http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt, 2007.

[3] Carl G., Kesidis G., Brooks R., and Rai S., "Denial of Service Attack Detection Techniques," *Computer Journal of IEEE Internet Computing*, vol. 10, no. 1, pp. 82-89, 2006.

[4] Chang C., "Defending Against Flooding-Based Distributed Denial of Service Attacks: A Tutorial," *Computer Journal of IEEE Communication Magazine*, vol. 40, no. 10, pp. 42-51, 2002.

[5] Chen R., Park J., and Marchany R., "A Divide and Conquer Strategy for Thwarting Distributed Denial of Service Attacks," *Computer Journal of IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 5, pp. 577-588, 2007.

[6] Cheswick R. and Bellovin M., *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison Wesley, 1994.

[7] Computer Emergency Response Team, http:// www.cert.org/advisories/ CA-2000-1.html, 2000.

[8] Computer Emergency Response Team, http:// www.cert.org/stats/ cert_stats.html, 2007.

[9] Criscuolo P., "Distributed Denial of Service Trin00," http: //ftp.se.kde.org /pub /security/csir/ ciac/ ciacdocs/ciac2319.txt, 2006.

[10] Cichardson R., "Computer Crime and Security Survey," http://www.crime-research.org/ news/ 11.06.2004 /423/, 2007.

[11] Dittrich D., Weaver G., Dietric S., and Long N., "The Mstream Distributed Denial of Service Attack Tool," http://staff. washington.edu /dittrich/misc.mstream.analysis.txt, 2007.

[12] Dittrich D., "The Stacheldraht Distributed Denial of Service Attack Tool," University of Washington, http://staff. washington. edu/dittrich /misc/stacheldraht.analysis.txt, 2007.

[13] Dittrich D., "The DoS Projects (Trinoo) Distributed Denial of Service Attack Tool," http://staff. washington.edu /dittrich/ misc/trinoo .analysis.txt, 2007.

[14] Dittrich D., "The Tribe Flood Network Distributed Denial of Service Attack Tool," http:// staff.washington.edu/dittrich/misc/trinoo. analysis.txt, 2007.

[15] Douligeris C. and Mitrokotsa A., "DDoS Attacks and Defense Mechanisms: Classification and State of the Art," *Computer Journal of Networks*, vol. 44, no. 5, pp. 643-666, 2004.

[16] Galli P., "DoS Attack Brings down SUN Grid Demo," http: //www. eweek.com/ article2 /0,1895, 1941574, 00.asp, 2007.

[17] Garber L., "Denial of Service Attacks Rip the Internet," *Computer Journal of IEEE*, vol. 33, no. 4, pp. 12-17, 2000.

[18] Gibson S., "The Strange Tale of the Denial of Service Attacks Against GRC.COM," http://grc.com/dos/grcdos.htm, 2007.

[19] Gonsalves C., Akamai DDoS Attack Whacks Web Traffic, http: //www. eweek.com/ article2 /0, 1895,1612739,00. asp, 2007.

[20] Gordon A., Loeb P., Lucysgyn W., and Richardson R., *CSI/FBI Computer Crime and Security Survey*, CSI Publications, 2006.

[21] Handley M., "Internet Architecture WG: DoS-Resistant Internet Subgroup Report," onlineathttp://www.communications.net/object/download/1543/doc/mjh-dos-summary.pdf. 2007.

[22] Haris B. and Hunt R., "TCP/IP Security Threats and Attack Methods," *Computer Journal of Communications Review*, vol. 22, no. 10, pp. 885-897, 1999.

[23] Haymarket Media, "Al-Jazeera Hacked in DoS Attack," http://www. itnews. com.au /newsstory. aspx?CIaNID=17603, 2007.

[24] Howard J., "An Analysis of Security Incidents on the Internet," *PhD Dissertation*, Carnegie Mellon University, 1997.

[25] ITworld. com, "CERT Hit by Ddos Attack for a Third Day," http://security.itworld.com/4339/ IDG010524CERT2/pfindex.html, 2007.

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

[27] McAfee, "Personal Firewall," http://www. mcafee.com, 2003.

[28] McCue A., "Bookie Reveals," http://software .silicon.com/ security/0, 39024655, 39121278, 00.htm, 2007.

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

[30] Mirkovic J., Arikan E., Wei S., Thomas R., Fahmy S., and Reiher P., "Benchmarks for DDOS Defense Evaluation," *in Proceedings of*

Military Communications Conference, pp. 1-10, Washington, 2006.
[31] Mirkovic J., "D-WARD: Source End Defense Against Distributed Denial of Service Attacks," *PhD Thesis*, University of California, 2003.
[32] Molsa J., "Mitigating Denial of Service Attacks in Computer Networks," *Doctoral Dissertation*, Helsinki University of Technology, 2006.
[33] Moore D., Shannon C., Brown D., Voelker G., and Savage S., "Inferring Internet Denial of Service Activity," *Computer Journal of ACM Transactions*, vol. 24, no. 2, pp. 115-139, 2006.
[34] Moore D., Voelker G., and Savage S., "Inferring Internet Denial of Service Activity," *in Proceedings of the 10th USENIX Security Symposium*, pp. 20-25, Washington, 2001.
[35] Oppliger R., "Internet Security: Firewalls and Beyond," *Computer Journal of Communications of the ACM*, vol. 40, no. 2, pp. 92-102, 1997.
[36] 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, 2007.
[37] Robinson M., Mirkovic J., Schnaider M., Michel S., and Reiher P., "Challenges and Principles of DDoS Defense," *Computer Journal of ACM SIGCOMM*, vol. 5, no. 2, pp. 148-152, 2003.
[38] Sardana A., Kumar K., and Joshi R., "Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP Domain," *in Proceedings of 3rd IEEE CS International Symposium on Information Assurance and Security*, UK, pp. 191-196, 2007.
[39] Sivakumar G., "Cryptographic Protocols and Network Security," http://www. cse. iitb. ac .in/~siva/talks /crypto.pdf, 2007.
[40] Tipton H. and Krause M., *Information Security Management Handbook*, CRC Press, 2004.

Monika Sachdeva has done BTech computer science and engineering from National Institute of Technology NIT, Jalandhar in 1997. She finished her MS software systems from BITS Pilani in 2002. Currently she is a PhD student in Department of Computer Science and Engineering at Guru Nanak Dev University, India.

Gurvinder Singh has been a meritorious student throughout his academic career. He did his MCA from Guru Nanak Dev University, Amritsar GNDU, Amritsar in 1996. He finished his PhD from GNDU, Amritsar in 2006. Currently, he is reader in the Department of Computer Science and Engineering, GNDU, India.

Krishan Kumar has done BTech computer science and engineering from National Institute of Technology NIT, Hamirpur in 1995. He finished his MS software systems from BITS Pilani in 2001. Recently in 2008, he finished his PhD from Department of Electronics and Computer Engineering at Indian Institute of Technology, Roorkee. Currently, he is an assistant professor at SBS College of Engineering and Technology, Ferozepur, India.

Kuldip Singh received the BE in electronics and communication and ME in electronics and communication and PhD in computer engineering degrees from University of Roorkee, Roorkee in 1968, 1970 and 1987 respectively. He is currently professor at Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, India. His research areas are parallel processing, computer networking, bioinformatics, continuing education and human resource development.