Layered Security Framework for Intrusion Prevention

Kamini Nalavade[1], B.B. Meshram[2]

[1] *Research Scholar,* [2]*Professor & Head*

Computer Engineering Department, V.J.T.I., Matunga, Mumbai

***Abstract*— Internet provides huge information and value to the users but at the same time access to the internet is prone to increasing number of attacks. Due to vulnerabilities in the network system, protecting network from malicious activities is prime concern today. It is important to analyse vulnerabilities and record them so that future attacks can be predicted. In this paper vulnerabilities which exist in the TCP/IP Model and the attacks which exploit these vulnerabilities are described. Existing defense mechanisms for the attacks are also discussed. We propose a security framework based on TCP/IP layered approach for defense against various network attacks.**

***Keywords*— Security, TCP/IP Model, Vulnerabilities, Attacks**

I. INTRODUCTION

The Information flow on Internet is constantly under various attacks because of vulnerabilities lying in the structure of networks. Hackers, intrusion, port scan, remote access, distributed denial-of-service (DDoS), virus, worm, email spam and many more are making the access to the information difficult and unreliable. Many defense methods and systems have been proposed in past. The attack detection is the crucial part of any defense system. Detecting known attacks is easier than detecting unknown and new attacks. TCP/IP Model has many flaws which makes it prone to attacks. Adapting totally new architecture for Internet for all users is difficult to implement. Because of this reason study of present architecture and the related vulnerabilities is important. This will also help in predicting future attacks.

As shown in Figure 1 the TCP/IP model is a collection of protocols for communication between computers. TCP/IP provides network link between remote computer's hardware and software irrespective of their manufacturers.

The TCP/IP model makes the information and resources sharing possible. Some of the important protocols of the model are Transmission control protocol(TCP), Internet protocol(IP), Address resolution protocol(ARP), Reverse ARP, Simple Mail Transfer Protocol (SMTP) etc. The Internet Protocol (IP) is a stateless protocol that transfers packet data from one machine to another; it uses 32-bit IP addresses, often written as four decimal numbers in the range 0–255, such as 172.16.8.93. Most Internet services use a protocol called Transmission Control Protocol (TCP), which is layered on top of IP, and provides virtual circuits by splitting up the data stream into IP packets and reassembling it at the far end, asking for repeats of any lost packets. Local networks mostly use Ethernet, in which devices have unique Ethernet addresses, which are mapped to IP addresses using the Address Resolution Protocol (ARP). There are many other components in the protocol suite for managing communications and providing higher-level services. Most of them were developed in the days when the Internet had only trusted hosts, and security wasn't a concern. So there is little authentication built in; and attempts to remedy this defect with the introduction of the next generation of IP (IPv6) are likely to take many years. [1]

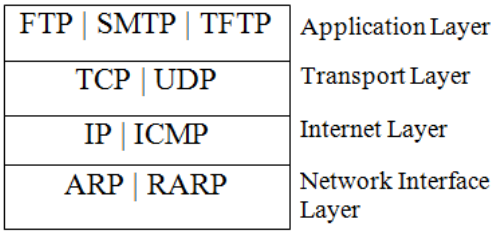

Figure 1 TCP/IP Protocol Suite

This paper presents the vulnerabilities, attacks and defense mechanisms for the layers of TCP/IP model.. The paper is organized as follows: In Section II we discuss the vulnerabilities in the TCP/IP model. Section III gives information about attacks due to vulnerabilities and defense mechanisms for the attacks. In Section IV we propose our security framework for detection and prevention against attacks. The last section summarizes this correspondence.

II. TCP/IP VULNERABILITIES AND ATTACKS

The current state of the TCP/IP network is vulnerable. The networks are prone to increasing number of attacks. It is very difficult to detect new attacks before subsequent damage is done. A computer network is a group of

Manuscript received June 5, 2011
Manuscript revised June 20, 2011

connected nodes. On one hand it needs to provide continuous service while on other hand it stores huge amount of confidential data. The remote access and unknown users increases the risk of being affected. Thus security is prime concern and focus today. Many of the protocols of TCP/IP stack were developed at an early stage when security was not prime concern. But modifications of these protocols are likely to take many years. That is the reason understanding of vulnerabilities of present model is important. Vulnerability is weakness or flaw in system which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker's access to the flaw, and attacker's capability to exploit the flaw. TCP/IP protocol suite has a number of vulnerabilities and security flaws inherent in the protocols. Those vulnerabilities are often used by crackers for Denial of service, session hijacking etc. Detailed description of vulnerabilities and attacks of every layer is given in the following sections.

2.1 Data Link Layer vulnerabilities and attacks- Data link layer is responsible for host to host data transfer. To identify any host physical address is required. ARP and RARP protocols provide the service of finding physical address from IP address and vice versa.

Address Resolution Protocol-

The Address Resolution Protocol (ARP) is a computer networking protocol for determining a network host's Link Layer or hardware address when only it's Internet Layer (IP) or Network Layer address is known. ARP finds hardware address by broadcasting a request. This request is read by all and the host who knows the MAC address replies back. Once the reply is received by host, it adds an entry to its ARP cache table. The major vulnerabilities lies in ARP broadcast and ARP cache entries. ARP cache entries can be modified, deleted or added by an unsolicited request. These types of attacks are known as ARP cache poisoning. The tools which are used for the attacks on ARP are ARO0c, ARPpoison etc.

2.2 Network Layer vulnerabilities and attacks- One of the most important protocol of TCP/IP model is IP (Internet Protocol) which handles important issues like addressing, routing in networks.

Internet Protocol-

The major vulnerability in most of the protocols of TCP/IP is lack of authentication mechanisms. This is the severe flaw which enables attacker to access the confidential information. IP spoofing is the attack which exploits the unauthenticated access vulnerability. Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host. Another major vulnerability in IP is the field source routing. If enabled it gathers network reconnaissance data which may be used by hacker for the attacks. As IP traffic is unencrypted, simple eavesdropping can gather lots of useful information like network topology, network infrastructure etc. Broadcast and multicast support in IP can cause denial of service. Flooding network resources with number of requests so that they will not be able to provide service to legitimate users is called as denial of service. IP spoofing makes detecting denial of service attacks worse as source IP address is spoofed, actual source cannot be caught. Packet fragmentation is one of the features of network layer IP protocol. Fragmentation is done if packet size is more than forwarding capacity. But unnecessary fragmentation may increase network traffic and ultimately may cause denial of service. The tools like Apsend, Ettercam, Nemesis, Hping makes the hacker's task easy. Packet capturing tools like wireshark, sniffit provides all the details of packets moving through the network. These packet capturing tools form the basis of most of the network attacks. Unauthenticated access to the traffic is the most harmful vulnerability of network layer.

2.3 Transport Layer vulnerabilities and Attacks- Traditionally TCP/IP Protocol suite has specified two protocols for the transport layer: UDP and TCP. Transport layer takes care of session management, connection establishment and release etc. TCP and UDP protocols are used for this purpose at transport layer.

A. Transmission Control Protocol

Transport layer provides a reliable, connection-oriented transport service to the upper layer protocols. As the Internet protocol (IP) does not provide reliable datagram service to network applications, this is of significance. One of TCP's primary features is a method of flow control and error correction called windowing. TCP has key characteristics like reliable connection setup and release, packet sequencing facility, retransmission of lost segments, multiplexing connections etc. Connection setup in TCP is done by 3 way handshake algorithm. This may cause SYN flood attacks or half open connection attacks. The attacker may send many connection establishment requests but will not acknowledge them. This makes the receiver's buffer full and it may not accept any new request which may be from legitimate users and can ultimately cause Denial of Service. As TCP is stateful protocol, TCP state mechanisms can be exploited to effect attacks. TCP state management mechanisms such as sequence numbers and TCP state flags can be manipulated

to effect attacks. Manipulation of TCP header flags can be used to hijack TCP connection. If attacker becomes successful in TCP sequence number prediction, he may control the session between server and legitimate users. TCP traffic is not supported by encryption facility. This enables many of the packet capturing tools to decode TCP data with ease this includes port information that can be useful to carry a malicious payload or to establish a covert communication channel with an external host.[2]

TCP denial of service can make use of TCP options, flags, SYN flooding. Land is an example of TCP denial of service. Land sets options in a TCP packet so that the source and destination IP address and source and destination port numbers are all identical. Earlier versions of TCP/IP used to process this type of packet and would crash. Tools like Juggernaut (1.02 patch) and hunt are making these once sophisticated attacks very easy. Some of the important tools which are used to effect attacks are Land, Bubonic, Targa3, Hping, Nemesis, Scapy, IPwatcher, Mstream etc.

B. User Datagram Protocol

User datagram protocol provides unreliable, connectionless service of transport layer. UDP provides services such as multiplexing connections, connectionless services. UDP lacks access and bandwidth control which causes denial of service and session hijacking. UDP traffic is unencrypted so anyone can capture the packets and decode it. In spite of a UDP header data checksum and unencrypted data, most of the UDP header fields are easily manipulated or reproduced. The ability of attacker to frame malformed UDP packet, increases the chances of UDP session or application data hampering. Difficulty in finding manipulated packets which cause denial of service is in inspection of UDP traffics at packet inspecting devices as UDP is connectionless. Though less common than IP and TCP covert data, the data portion of UDP packets does provide some facility for tunnelling covert data in and out of network.

2.4 Application Layer vulnerabilities and attacks:

As in TCP/IP, the Application Layer contains all protocols and methods that fall into the realm of process-to-process communications across an Internet Protocol (IP) network. The protocols explicitly mentioned in RFC 1123 (1989), describing the Application Layer of the Internet Protocol Suite are FTP, TFTP, Telnet, SMTP, DNS, BOOTP, SNMP,CMOT. In this paper, we present vulnerability and attack analysis of SMTP protocol.

Simple Mail Transfer Protocol-

While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically only use SMTP for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP) or a proprietary system (such as Microsoft Exchange or Lotus Notes) to access their mail box accounts on a mail server.

Weakness in authentication mechanisms and lack of complex access control are the most exploited vulnerabilities of SMTP. Most mail servers are configured to support anonymous access. SMTP supports anonymous 'write' transactions. SMTP delivery status notification has vulnerabilities which are exploited to construct denial of service attacks. SMTP Message headers contain a wealth of useful topology and reconnaissance data for attackers. Like IP packets, SMTP message contains all useful information necessary to ensure successful delivery and tracking of an individual mail message. MIME is used to encapsulate non ASCII or binary data in mail messages to facilitate transmission of attachments containing application contents. Attacker may embed malicious attachments in MIME messages. Some of the SMTP Commands are considered insecure because they provide data to attackers which may be useful for attacks. For example ETRN allows for client side processing of mail queue and creates way to server or system penetration. The SMTP protocol does not encrypt mail content and does not support traffic privacy. Attacks against mail privacy and confidentiality constitute largest class of SMTP and mail protocol attacks. SMTP servers are often present on network and are associated with other applications on a private network. [2]

Mail bombing is the activity of sending large number of emails to a single mailbox with the intention of denial of service. Mail spamming is sending unsolicited mail to a large number of recipients via a mailing list. Spamming and mail bombing involve elements of spoofing and message header manipulation. The technical sophistication of attacker may reveal the source's true email account. Various tools can be employed to construct a mail bombing attack. Many of the tools allow for construction of SMTP headers and data and provide variety of spoofing options. Most popular SMTP attack tools include Linsniffer, MailSnarf, Netcat, Telnet etc.

III. TCP/IP DEFENSE AGAINST ATTACK

These attacks attempt to exploit the weaknesses present during the implementation The defense techniques popularly used are intrusion detection system, intrusion prevention system, firewalls, Traffic monitoring etc. The countermeasures suggested in this paper may vary according to specific system, the threat model associated with the organization and sensitivity level of data.

Defense against ARP attacks

Increase in MAC table entry timeouts in switches can minimize switch leakage. If only encrypted terminal sessions/file transfers are allowed the unauthorized packet manipulation can be minimized. Using arpwatch to keep track of ethernet/IP address pairings and monitoring may control arp denial of service. Use of static ARP tables will reduce the ARP cache poisoning.

Defense against IP attacks

Detective controls such as IDS can be used to identify types of IP-based attacks. Institution of security protocols like IPSec that can compensate for security vulnerabilities in the IP protocol. To protect network reconnaissance data deny source routing at gateways and firewalls. Institution of spoof protection mechanism and traffic monitoring is required at firewalls and other access control devices to prevent IP spoofing attacks.

Defense against TCP & UDP Attacks

Activation of SYN flood protection on firewalls and perimeter gateways can provide protection from TCP denial of service. Monitoring network traffic using network and host based Intrusion detection system can also be useful. Stateful firewalling is another solution for TCP attacks. TCP sequence number prediction can be avoided by randomly changing the sequence number generation algorithm. To avoid UDP denial of service attack, disable unnecessary UDP services. Institute stateful firewalling and monitor UDP traffic using network based IDS for protection against attacks. Employ network controls to guard against UDP packet flooding attacks.

Defense against SMTP Attacks

Antispam/ antirelay controls are intended to provide protection against mail relaying, mail spamming and various forms of related mail attack [2]. Relaying controls prevent an administered mail server from accepting mail bound for other mail domains. Many SMTP servers allow administrator to identify a list of IP restrictions to deny access to the SMTP server for a specified list.

Modern SMTP submission servers often include content-based security and denial-of-service defense mechanisms such as virus filtering, size limits, server-generated signatures, spam filtering, etc. Implementations of BURL should fetch the URL content prior to application of such content-based mechanisms in order to preserve their function.

Clients that generate unsolicited bulk email or email with viruses could use this mechanism to compensate for a slow link between the clients and submit server. This makes it more important for submit server vendors implementing BURL to have auditing and defenses against such denial-of-service attacks including mandatory authentication, logging that associates unique client identifiers with mail transactions, limits on reuse of the same IMAP URL, rate limits, recipient count limits, and content filters. [4]

IV. PROPOSED SECURITY FRAMEWORK FOR PROTECTION

Some of the major advantages of layered approach are interoperability, flexibility, scalability, abstraction and easy implementation. Layered approach can be observed in TCP/IP and OSI models. For example routers at network layer, switches at link layer. The layered approach of TCP/IP is demonstrated in figure 2.

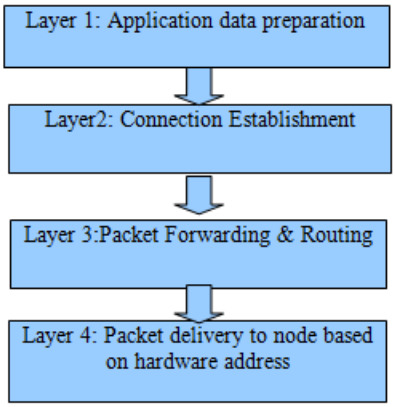

Figure 2 Layered Architecture of TCP/IP

The different devices implement security at each layer. The device specific exploits are also matter of concern like routing table poisoning, ARP cache poisoning etc. In many of the security systems confidentiality, availability and integrity are considered in isolation of each other. Many of the protection mechanisms work at individual layer. In our proposed framework we combine layered approach of TCP/IP and security objectives. As security is implemented individually at protocol level, the combining result of each protocol layer security will be more effective. If attack is not detected at one layer, it should be detected at next layer. Also the application layer should be supported by feedback of previously detected attack and action. This will reduce the network traffic and occurrence of same attack again.

Intrusion detection started in around 1980s. Intrusion detection systems are classified as network based, host based or application based depending upon their mode of deployment and data used for analysis. Intrusion detection system can also be classified as signature based or anomaly based depending upon their attack detection method. The signature based systems are trained by extracting specific patterns from previously known attacks while the anomaly based systems learn from the normal data collected when there is no anomalous activity [25]. Another approach is to consider both the normal and known patterns for training a system and then performing classification on the test data. Such a system incorporates the advantages of both the signature-based and anomaly based systems and is known

as the Hybrid System. Hybrid system can be very efficient subject to the classification method used and can also be used to label unseen or new instances as they assign one of the known classes to every test instance[24]. However data requirement is also a concern for these systems as they require completely anomalous and attack free data, which are not easy to ensure. Large amount of work is done in the area of Intrusion detection and number of techniques using data mining approaches has been described in order to detect an intrusion. But prevention of attacks is of equal importance to detection.

In most of the security systems attack is detected when it has already performed the damage. For prevention of attacks early detection and stopping the propagation in the network is very important. In this framework our approach is to try to find the attack as soon as it originates instead of permitting it to propagate and detect at end level. As TCP/IP follows layered approach and we know many of vulnerabilities of TCP/IP. Advantages of layered architecture of TCP/IP motivated us to use the same approach for recovery from these vulnerabilities. Based on these factors we propose a security framework of Intrusion protection system to ensure network security. Intrusion detection and prevention.

Intrusion detection starts with instrumentation of a computer network for data collection. Pattern-based software 'sensors' monitor the network traffic and raise 'alarms' when the traffic matches a saved pattern. Security analysts decide whether these alarms indicate an event serious enough to warrant a response. A response might be to shut down a part of the network, to phone the internet service provider associated with suspicious traffic, or to simply make note of unusual traffic for future reference. If the network is small and signatures are kept up to date, the human analyst solution to intrusion detection works well. But when organizations have a large, complex network the human analysts quickly become overwhelmed by the number of alarms they need to review. This situation arises from ever increasing attacks on the network, as well as a tendency for sensor patterns to be insufficiently selective (i.e., raise too many false alarms).

In this framework we try to achieve the three main security objectives by implementing attack occurrence check at each layer and predicting occurrence of attack by applying data mining algorithm on network traffic data.

As shown in figure 3 we propose that intrusion protection system have three main modules namely preprocessing, data mining and recommendation. Preprocessing module gathers information, process it, cleanses it and stores it in structured format. Updating the data is also role of preprocessing module. Data mining module applies mining algorithm on data produced by preprocessing module. The mining results are used by recommendation module for decision making and for suggesting action to the application. Results are stored in the database for use by applications while preparing their data. The preprocessing modules have complex structure. Here we try to achieve basic security objectives by checking confidentiality, availability and integrity. The availability objective can be achieved by not flooding the recipient with connections.

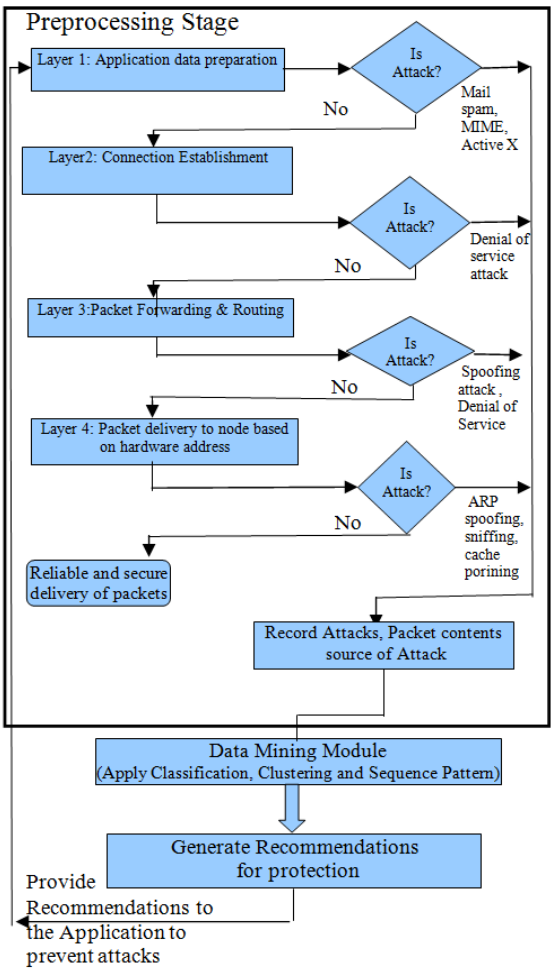

Figure 3 Proposed System Architecture

As connection establishment is done at transport layer, availability attacks can be detected at Transport Layer. The major availability attack is denial-of-service. Connection flooding or SYN flooding may cause denial-of-service, as there are other possible reasons also. If some network control mechanism is applied at transport layer then denial of service can be controlled. Confidentiality is required to be checked during transmission at every router before forwarding the message. Spoofing or session hijacking attacks are affecting the confidentiality of the message as receiver is getting the data from unauthorised person. Usually these attacks take place when a legitimate user sends some information to the recipient. But attacker in between captures the packet and see all the information including source, destination, data part etc. There are many

techniques suggested by many researchers for detection of spoofing attack like IP Traceback [6], use of hop count filtering field of IP header[7] etc. any of these can be implemented at network layer. At data link layer possibility of ARP attacks is more. To control these attacks use of network monitoring tool and static ARP cache table is required. Implementation of network monitoring, capture and analysis can be done at link layer. These precautionary measures will be implemented at individual layer. Also the information of attacks which are detected at any of the layer are received by data mining module and then passed on to the recommendation engine for action. This model gives personalised security to each host as the attacks differ from host to host. Also applying same strategy to all the nodes for attacks may not be effective. Applying data mining techniques helps in attack differentiation and decision making to the host.

V. CONCLUSION AND FUTURE WORK

As computer network is continuously evolving, the numbers of attacks on the system are also increasing. As attack increases network traffic problems arises. It is important to detect attack at the earliest stage to reduce the further damage. In this paper we have addressed the vulnerabilities and possible attacks at each layer of TCP/IP. The existing defense mechanisms for the attacks are also given. Further we have proposed a framework for intrusion protection and discussed its advantages compared to existing system. Though the architecture of the system is complex, layered approach framework can make implementation easy. We are currently analysing vulnerabilities of security protocol and as part of our future work we plan to implement this framework as a single system. Several areas remain to be addressed such as automated network traceback, robustness of model.

VI. REFERENCES

[1] Roger Needham And Butler Lampson. , "Network Attacks and Defense", Pg no. 370

[2] Sousan Young, Dave Aitel, "The Hackers Handbook", Auerbach publication

[3] Kapil Kumar Gupta, Baikunth Nath, Kotagiri Ramamohanrao, "Layered Approach using Conditional Random Fields for Intrusion Detection", IEEE Transactions on dependable and secure computing, vol. 7, no. 1, january-march 2010

[4] Kapil Kumar Gupta, Baikunth Nath, Kotagiri Ramamohanrao, "Network Security Framework" , IJCSNS International Journal of Computer Science and Network Secuirty, Vol 6, N0 7B, July 2006.

[5] C.Newman, RFC 4468, May 2006.

[6] Stefan Savage, David Wetherall Anna karlin and Tom Anderson, "Network Support for IP Traceback", IEEE/ACM Transactions on Networking Vol 9, No3, June 2001.

[7] Haing Wang, Cheng Jin and Kang Shin, "Defense against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM Transactions on Networking, Vol 15, No1, February 2007

[8] R. Agrawal, T. Imielinski and A. swami. "Mining association rules between sets of items in large databases". In proceedings of the 1993 International conference on Management of Data , (SIGMOD 93), ACM Press Volume 22Issue 2, 1993, Pages 207-216.

[9] W. Lee and S. Stolfo, "Data mining approaches for intrusion detection", In the proceeding of 7th USENIX Security Symposium, 1998, pages 79-94

[10] D. Dennigs, "An intrusion detection model", IEEE Transactions on software engineering vol no.2 1987.

[11] TCP/IP Illustrted Volume 1(The protocols), W. Richard stevens, Addison- Weseley, ISBN 0-201-63346-9

[12] Douglas E. Comer, "Internetworking with TCP/IP ", Vol 1, Prentice Hall publication,

[13] www.insecure.org

[14] Skoudis, Ed. Counter Hack, "A step by step guide to computer attacks and Effective defenses", Prentice Hall.

[15] Oludele Awodele, Sunday Idowu,*Omotola Anjorin, and Vincent J. Joshua*, "A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and PreventionSystem (IIDPS)", **I**ssues in Informing Science and Information Technology Volume 6, 2009, Page no. 631.

[16] Abraham Yaar, Adrian Perrig and Dawn Song, "StackPi: New Packet Marking and Filtering Mechanisms for DdoS and IP Spoofing Defense", IEEE journal on Selected Areas in Communications, Vol 24, No 10, October 2006.

[17] Haing Wang, and Kang G. Shin, "Transport Aware IP routers: A built in Protection Mechanism to counter DdoD Attacks, IEEE Transactions on Paraller and Distributed Systems", Vol14, No 9, Sepember 2003.

[18] Cliff C. Zou, Nick Duffield, Don Towsley and Weibo Gong, "Adaptive Defense Against Various Network Attacks", IEEE journal on Selected Areas in Communications, Vol 24, No 10, October 2006.

[19] Joao Antunes, Nuno Neves, Miguel Correia, Paulo Verissimo, Rui Neves, ""Vulnerability Discovery with Attack Injection, IEEE transactions on Software Engineering, Vol 36 No. 3, May/June 2010.

[20] Zhenwei Yu, Jeffrey J. P. Tsai and Thomas Weigert, "An automatically Tuning Intrusion Detection System", IEEE Transactions on Systems, Man and Cybernetics- PART B: CYBERNETICS, Vol 37, No. 2, April 2007.

[21] CERT Coordination Center , Denial-of-service Tools, IP spoofing tools, Smurf Attack http://www.cert.org

[22] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP source address spoofing", RFC 2827, May 2000

[23] Jelena Mirkovic, Peter Reither, "A Taxonomy of DDOS Attack and DDoS Defense mechanisms ", In proceedings of the 2nd ACM SIGCOMM Internet Measurement Workshop, November 2002.

[24] Kapil Kumar Gupta, Baikunth Nath, Kotagiri Ramamohanrao, "Layered Approach Using Conditional Random Fields for intrusion detection" ,IEEE Transactions on Dependable and Secure Computing, VOL 7, No. 1, January-March 2010.

[25] R. Bace and P. Mell, Intrusion Detection Systems, Computer Security Division, Information Technology Laboratory, Nat Inst. of standards and Technology 2001.

Kamini C. Nalavade received the B.E. degree in computer science and engineering from the SGGS, College of engineering and technology, Nanded in 2001 and M.Tech degree in computer engineering from Veermata Jijabai Technological Institute (VJTI), Mumbai in 2007. She is currently PhD student in the department of computer engineering, VJTI, Mumbai. Her research interest includes intrusion detection, network security, data mining and data privacy.

Dr. B. B. Meshram is currently professor and Head of Computer Technology Department of Veermata Jijabai Technological Institute (VJTI), Matunga, Mumbai (INDIA). His areas of interest include Object oriented database management systems, Computer network security and multimedia systems. He has published more than 40 papers in National & International Conferences & refereed Journals.