ANALYSIS OF SECURITY ASPECTS FOR DYNAMIC RESOURCE MANAGEMENT IN DISTRIBUTED SYSTEMS

V.S. Tondre[1], Dr. V.M Thakare[2], Dr. S.S. Sherekar[2] and Dr. R.V. Dharaskar[3]

[1]B. B. S. C. Amravati, (M.S.), India.
[1]varshatondre@rediffmail.com,
[2] Deptt. Of Computer Science, S.G.B. Amravati University. Amravati, (M.S.), India.
[2]vilthakare@yahoo.co.in,
[2]ss_sherekar@rediffmail.com,
[3]M.P.G.I., Nanded, (M.S.), India.
[3]rvdharaskar@rediffmail.com

Abstract

Millions of people all over the world are now connected to the Internet for doing business. Therefore, the demand for Internet and web-based services continues to grow. So, need to install required infrastructure to balance the computing. In spite the success of new infrastructure, it is susceptible to several critical malfunctions. Therefore, to guarantee the secure operations on Network and Data, several solutions need to be developed. The researchers are working in this direction to have the better solution for security.

In distributed environment, at the time of management of resources both computing and networking, resource allocation and resource utilization, etc, the security is most crucial problem. In this paper, an extensive review has been made on the different security aspect, different types of attack and techniques to sustain and block the attack in the distributed environment.

Keywords

Anomaly discovery, Firewall, Client-Server, Internet, distributed system, Security.

1. INTRODUCTION

Now, Security has become a critical issue for the world of network. To execute and later in business, the Internet has budged from alleviate to a mission-critical platform. As the Internet application overcome, security problems due to intruders arise.

Security is vital for distributed and collaborative applications such as video-conferencing, clustering and replication applications, which operate in dynamic network environment and communicate over secure network i.e. Internet [1].

Firewalls are important factor in the network security. With global Internet connection, researchers now concentrate towards the network security. In which rate the usage of network increased, with the same rate threat of network attacks are also increased. Firewall plays an important role in network attacks. It became an integrated element not only in enterprise network but also in small-size and home network [2].

DOI : 10.5121/ijcseit.2011.1501

In recent years, firewalls are extensively implemented in the Internet, to chunk unwanted traffic. So, many factors are used to make firewall configuration complex, which includes the introduction of new protocols and the regular discovery of worms.

2. CLASSIFICATION OF SECURITY ISSUES

The paper focused on two types of Security Issues

1. Security for Data.
2. Security for Network.

3. METHODOLOGIES OF SECURITY FOR INTERNET AND DATA

In this section, discussion is on the different security issues of Internet and Data.

3.1 Security for Stored Data

Many times it is essential for many applications to store data for long-term and retrieve it for later use. These applications may be single user applications storing personal information or multi-user joint applications, which allow users to share stored data. In addition, these applications may run on computers, which vary form desktop to mobile and handheld devices. Here, it required to provide the service application, which is easy to manage, store and access sensitive information. The storage service design must contain the qualities as data should be highly available, quickly accessible to distributed clients, access to the private and protected data should be controlled, privacy and integrity of the stored data should not be negotiated, and these requirements should be met even when some numbers of servers in the secure store are cooperation by the adversary.

The [3], present a design and analysis of a distributed data store, which provide the security and required performance. It is a combination of two famous techniques, replication and secret sharing. It is presented in the form of architecture shown in fig. 1. In this architecture, the store is implemented by a set of n servers. Clients make read and write operations with subset of servers. It assume the public key infrastructure, each client and server node has a private key for which the public key is well-known, together with this client and servers also discuss symmetric keys once in a while to exchange messages. Consequently, all communication channels are secure against eavesdropping, modification and replay attacks. At each receiver, requests are authorized using access control lists, which are updated securely and in a timely fashion by a system administrator, using separate service.

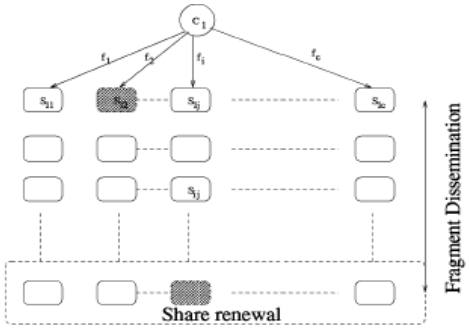

Fig. 1. Secure store architecture

3.2 Anonymity in P2P System

In P2P system, one essential problem is to implement the trust of the data stored in the system and security of the peers. Each peer can work as a provider, as a requester and a publisher. Many times publisher can distribute its document to other provider peers in orders to oppose control and document can also be cached in some non-producer peers. Depending on the certain conditions, application and users of the system may require different levels of anonymity.

To achieve the mutual anonymity between the initiator and responder with high efficiency, authors in [4] suggested two methods. First method for trusted server, which is presumes the existence of trusted index servers. The index server prepares a convert path for initiator and responder, which reduce the operation and communication overhead. In the above method [4] suggested two new techniques: center-directing, where encryption cost is independent of the length of the convert path, and label switching, which eliminates potentially excessive messages in center directing. In second method, it assumes P2P settings. By using anonymity protocol what is called shortest-responding, reduces the communication overhead while preserving mutual anonymity.

3.3 Robust Contributory Key Agreement

The basic security services needed in the Internat network are data secrecy, integrity and entity authentication. These services are not achieved without secure, efficient, and robust group key management.

In the [1], it provides a robust and secure group communication, which offers Virtual Synchrony (VS) semantics. It gives in three steps:

1. The first part is robust contributory key agreement protocols, which are flexible to any finite sequence events. The protocol is based on Group Diffie-Hellman (GDH) key agreement.

2. Reliable group communication service (GCS) and robust key agreement is combined to provide robust and secure group communication service.

3. An insight into the cost of adding security services to GCS, focusing on group key management costs. The implementation of a secure group communication service-secure spread-based on optimized robust key agreement protocol and the Spread group communication systems. It provides the strong security properties just like the group key agreement.

3.4 Modeling and Management of Firewall Technique

Firewalls are used to secure network against attacks and unauthorized traffic by filtering out unwanted traffic coming into or going from the secured network. The decision of the filtering is taken according to a set of ordered filtering rules. These rules are based on the predefined security policy.

To analyze the firewall policy and design management techniques, firewall rule relations are necessary. Such techniques are anomaly discovery and policy editing. Authors in [2] presented a formalization of filtering rule relations. In this process, first determine all possible relations, which are related to packet filters. Define all possible relations, which may exist between filtering rules and show that no other relation exists. All the relations are based on comparing the network fields of filtering rules, independent of the rule actions.

3.4.1 Anomaly discovery

A firewall policy anomaly is defined as the existence of two or more filtering rules that may match the same packet, or the existence of a rule that can never match any packet on the network paths that cross the firewall. The following different types of anomaly may exist among filtering rules in one firewall.

- Shadowing Anomaly–A rule shadowed when a previous rule matches all the packets that match this rule
- Correlation Anomaly – Two rules are correlated if they have different filtering actions, and the first rule matches some packets that match the second rule and the second rule matches some packets that match the first rule.
- Generalization Anomaly – A rules is a generalization of a preceding rule if they have different actions, and if the first rule can match all the packets that match the second rule.
- Redundancy Anomaly – If there is another rule, which produces the same matching and action is called as redundant rule.
- Irrelevance Anomaly – A filtering rule in a firewall is irrelevant if this rule does match any traffic that may flow through this firewall.

The fundamental idea of discovering anomalies is to determine if any two rules coincide in their policy tree paths. If the path of a rule coincides with the path of another rule, there is a potential anomaly, which can be determined based on the firewall anomaly definition. If rule paths do not coincide, then these rules are disjoint and they have anomaly.

3.4.2 Firewall policy editing

It contains new security requirements and network topology changes. However, editing security policy cannot easy compare to creating new one. As all the rules of firewall are in ordered, a new rule must in place in a particular order to avoid the anomaly. The same thing is applied for modification and removal. Using policy editor, administrator needs no prior analysis of the firewall policy rule in order to insert, modify or remove a rule [4].

3.5 Firewall Optimization Techniques

Firewalls means implement network policy. When communication access privileges between network and host are define, firewalls are best for network policy. The access privileges are most typically involved network, protocol, session and host restrictions. Firewalls implement these policies by mediating the communication among hosts in different networks. It checks the packet's header against a set of user-defined rules and forwards the packet if it is desired /undesired. Through, inspection and filtering, firewalls can catch doubtful packets and prevent them from passing through. In this way, it helps to improve network security.

The general framework suggested in [5], for rule based firewall optimization. In framework, it captures the semantics of ACL (Access Control List) in terms whether each packet is accepted or rejected. To accomplish this, it divides packet space into independent partitions to correctly consider the changed set of packets matched by rules as the packets are processed within an ACL. Additionally, it compared to existing approaches. In this way, this model is able to find the optimal rule for reordering. Thus, it can also be used to compare and evaluate other optimization approaches and recognize their practical benefits and limitations. Authors in [5], focuses on the optimality of rule orders generated by the optimization rather than running time of the optimization algorithms because its direct impact on firewall performance and running time optimization does not affect firewall performance and one-time offline process.

The process used for firewall optimization:

1. It provides an algorithm, which given an ACL and a traffic profile, produces the optimal reordered rules. It is based on a novel rule-based partitioning of the packet space and reduction to integer programming.

2. It formally establishes the correctness of the algorithm. It uses a semantic formalization of firewalls and its equivalence. An equivalence argument connecting this formalization with the reduction to integer programming.

3. It provides an evaluation framework for rule based firewall optimization techniques. It is specially used to empirically evaluate two representative heuristic algorithms. New one additional introduced production firewall configuration, which is effective for understanding the tradeoffs of firewall optimization techniques.

3.6 Security and Solutions for P2P

In recent years, with the file sharing applications, peer to peer (P2P) overlay network become quite popular. This P2P networks are also used for content distribution and Voice over IP (VoIP). P2P overlays can be divided into two types as structured and unstructured. The unstructured P2P overlay network is simple and search operations are inefficient. On other hand, structured P2P overlays use Distributed Hash Table (DHT) to perform directed searches, which lookups more efficient in locating data. In P2P real time communications several attacks, security issues and solutions are discussed in [6].

A DHT is a distributed system, used to implement hash table. It used for efficiently storing and retrieving key value pairs. It is also used hash functions to map keys on network nodes. In P2P, users are directly involved in the condition of the service and due to complete lack of control, several numbers of attacks caused by spiteful peer inside the overlay.

There are several reasons to do attacks such as financial gain, personal enmity or for fame. There are very few cases of denial of service attacks for extortion in the client-server model. Resources are another important factor in the attacks. It is also used to find the nature of the attack. An attacker may use the Internet relay channel and launch distributed denial of service attack against another node. The victim of the attack may be an individual node such as a node or an entire overlay service. It may happen that the malicious node may start misbehaving as soon as it enter in the overlay or it could follow the rules of the overlay for finite amount of time and then attack.

4 ANALYSIS AND DISCUSSION

In this section all the above techniques of the security for data and network are analyzed and discussed.

4.1 Design provided in [1], gives greater flexibility to get security and performance needs compared to either a pure replication or a pure secret sharing scheme. The design of the system does not depend on any specific choice for these schemes. One can use secret sharing or share renewal scheme that satisfies certain requirements, as appropriate for protocols.

4.2 To build secure and trusted P2P systems, it is the need to provide a reliable and efficient anonymity protection among peers [2]. The suggested shortest responding protocol is designed for pure P2P systems, while mix-based, center-directing and label-switching protocols are

specially designed for hybrid P2P system to achieve mutual anonymity. Shortcut-responding protocol is good for the pure P2P system. Moreover, the number of middle nodes in convert path is used to control its cost. The label-switching protocol is best for efficiency when the storage space is not concern. If it concern, then center-directing protocol is good one. If the large number of middle nodes is required for strong anonymity, center directing and label switching are the best.

4.3 It is very difficult to freeze security protocols to make them robust to asynchronous network events. The above-mentioned in [3] protocols are used to design secure group communication services. Group communication membership and ordering guarantees are preserved by integrating GDH key protocol and GCS supporting Virtual Synchrony.

4.4 Firewall security also requires proper management to provide the security service. Therefore, the firewall policy advisor provides a number of new tools for filtering and protecting the firewall from anomalies. Those tools are policy analyzer and policy editor, which are very effective for managing firewall policies in real life networks [4].

4.5 The general framework for evaluating optimization techniques for rule based firewalls. It divides the packet space into partitions where all the packets in any given partitions, which matches all the packets in a given partition with the same set of firewall rules. For each partition, the framework calculates the cost for the firewall to process all the packets in the partition based on traffic profile. The framework formulates firewall optimization as an integer programming problem and developed a firewall optimization technique [5].

4.6 As DHT's are designed in such a way that it could work in environment characterized by high mix rates, they are fault tolerant and less susceptible to denial of service attacks than centralized solutions. Moreover, some of the major common security issues such as integrity and confidentiality are addressed on the endpoints. Thus, the solutions are common in distributed and centralized environments. In this way users are directly involved in the provision of service and due to the complete lack of control, P2P network may subject to a number of attacks because of malicious peer inside the overlay [6].

5 INTERNET ATTACKS AND DEFENSE TECHNIQUES IN DISTRIBUTED SYSTEMS

In this section, only Internet attacks and defense techniques are discussed.

5.1 Transport-Aware IP Routers : A Built in Technique

On the Internet, Denial of Service (DoS) attacks are renowned to hard to defend. New recent occurrence of, distributed DoS (DDoS) attacks make it more difficult for sufferer to block and trace back the attacking sources [7].

At the end-server, limited network sources are available to Internet users like bandwidth, buffer and processing power of routers. The weakness of the network resources makes DDoS attackers easy to attack on traffic to control network. Sufficient service differentiation and resource isolation at IP routers provides not only the network quality of service at end users, but also to counter DDoS attacks as a powerful built in protection mechanism inside the Internet.

5.1.1 Description of attack

A DDoS attack system is usually be described as hierarchical model, where attacker controls a

handler (master) i.e. orders the group of agents (slaves) to flood the bogus packets to the victim. The master sends the control packets towards the preciously compromised slaves, ordering them to target a given victim. The slaves then generate and send high-volume streams of flooding messages to the victim with the fake source addresses the victim cannot locate the attackers.

To prevent the DDoS attacks and provide service differentiation, in [7] suggested a complicated resource management schemes at end servers, i.e. a transport-aware IP (tIP) router architecture which, provide fine-grained service differentiation and resource isolation among thinner aggregates without compromising scalability.

5.2 IP Traceback-Based Intelligent Packet Filtering

When DDoS attacks against the renowned web sites like yahoo, Amazon, then these sites are damaged and defenseless, i.e. the services of the web sites are unavailable for hours or even days.

5.2.1 Working of DDoS:

A human rival first compromises a large number of Internet-connected hosts by using network software weaknesses, such as buffer overflows. Then, DDoS software TFN (Tribe Flood Network) installed on the system. These hosts will later commanded by the rival to continuously send large volume of traffic towards a victim or network. The victim is overwhelmed by traffic that it can provide little or no service to its legitimate clients.

Suggested technique in [8], is a protocol-independent DDoS defense scheme which is able to improve the throughput of the legal traffic during the DDoS attack. In this technique, it controls on and extends the IP traceback techniques to collect the information i.e., whether or not a network edge is on the path from an attacker. According to the preferences, it filters the packets, which are emblazoned with the mark. It filters out most of the traffic from attackers since each and every edge on an attacker's path to the victim is infected.

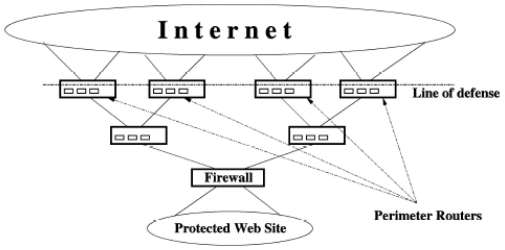

Fig. 2 system model to alleviate the attack

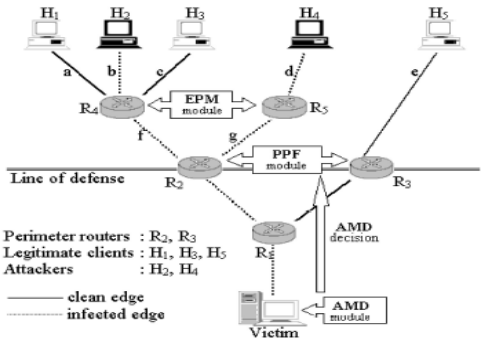

Fig. 3 example network as seen from the victim

As suggested in system model of [8] shown in above fig. 2 to alleviate the attack, proper action needs to be taken at upstream routers. So, the protected network is connected to the wide area network (WAN) through a gateway access control device i.e. firewalls, VPN. It forms a line of defense that will jointly inspect packets going through them. To control on attackers path and extend IP traceback technique to find out whether or not a network edge is on the path of the attacker. The union of the modules with the actual physical devices as shown in fig. 3 network we seen from the victim.

5.3 Perimeter-Based Defense against High Bandwidth

Perimeter-based defense mechanisms is a technique suggested in [9], it allows Internet Service Provider (ISP) to provide an anti DDoS service to its customers. The edge of the routers of an ISP forms a perimeter separating the customer networks from the rest of the network. There are two types of perimeter-based defense mechanism.

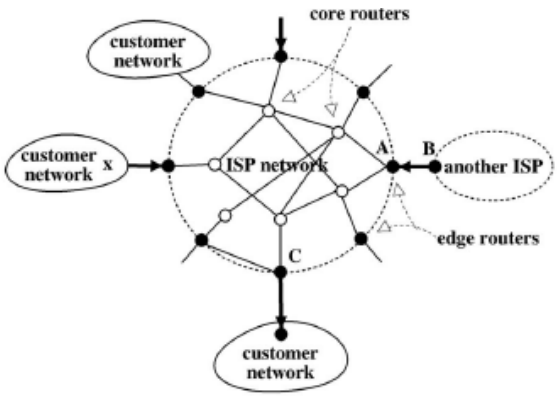

Fig. 4 Edge routers from a defense perimeter against DDoS

The first perimeter-based defense mechanism is DPM (Defense Perimeter Based on Multicast)as shown in fig.4. In this technique the edge, routers of an ISP form a designated, restricted multicast group. The address of the group is local to the ISP and any external join requests must be rejected.

In the specified DDoS attack, the edge router connected to the victim network, which helps to plan the defense, is called as the coordinator. It planes to initiate defense process after it receives an anti-DDoS request, which contains the description of the attack aggregate and a desirable rate of the aggregate. This request may be produce by the server under attack by the management console from the side of customer/ISP or firewalls, routers and intrusion detection devices based on reconfigured policies. After that the coordinator begins DPM by instructing the edge routers to install rate limit filters for the attack aggregate. Then it monitors the exit rate of a aggregate and periodically multicast a new to the other edge routers, which update their rate limits for aggregate, according to the received base rate. This process repeats until the exit rate converges to the desirable rate. The main goal of the DPM is to reduce the exit rate to a range close to the desirable rate and to minimize the amount of legitimate traffic i.e. mistakenly blocked by the edge routers.

The main disadvantage of DPM is that, even when there is only one flooding source, the rate-limit filters are temporary placed on all edge routers, however, most are removed after a period since they do not cause any packet to be dropped. This problem is overcome by using the second mechanism.

It is DPIT (Defense Perimeter Based on IP TraceBack). In this method, it generates less rate-limit filters at the cost of additional overhead at the coordinator. It finds the flooding sources by IP traceback.

5.4 Statistical Method to Trace Back Attackers

The probabilistic marking method is improved in [10], by precisely identifying the locations of the DDoS attackers. Following are the steps of the method:

1. Authors presented an effective method to allow a victim site to deduce the local traffic rates of all participating routers in an attack graph.

2. Also gives the theoretical framework to determine the minimum stable time, which is the minimum time required to accurately determine the local traffic rates of all the participating routers. One important thing is the lower value of the earlier a system administrator can determine the locations of the attackers.

3. An effective traceback methodology is given for a general network topology and different attack patterns.

5.5 Securing P2P against Identity Attack

Structured P2P overlay can simplify data storage and management for a verity of large scale distributed applications. Thus, the usefulness of the infrastructure has been validated by study of real world use of structured overlay applications [11]. Still, these applications infrastructures are susceptible to numerous critical spiteful attacks. One of them is Identity attack, which allows the spiteful peer in the network to capture application request and assume the responsibility of any application component.

Fig.5. the Identity Attack. 1023 sends a message towards key 3222. Before the message reaches the root 3223, an attacker intercepts it and responds as the root.

Identity attack: In structured P2P application used Key-Based Routing (KBR) to assign application components such as traffic indirection, storage servers or measurement servers to the live node in the network. An attacker can take control and maintain KBR messages as its own. Attacker, make use of KBR information, that each node only sees a small subset of the overlay members. It is known as Identity attack. Any spiteful peer on the path of a KBR message can respond to the source code and maintain, as it is request's destination. The undetected attacker takes a control of particular key and its related applications. Multiple attackers can jointly perform stronger attacks. That is, separate the node from the network and effectively perform the manual partitioning of the overlay.

Nodes detect the identity attack through the generation and timely distribution of self-verifying, "Existence proofs". The overlay nodes periodically, sign and distribute these proofs on behalf of well-defined regions of the namespace they reside in [11]. For each section, a small number of randomly selected proofs are stored and provide them on request through proof manager. Existence proofs are digitally signed certificates.

In [11], Self-verifying evidence of an attack is the first mechanism, used to track down and mark attackers. It also allowing overlay peers to locate and avoid attacker's node in favor of more reliable alternative routes. Second mechanism is to track attackers via blacklist; it verifies the valid evidence of the interested third parties in the network. If it found, adds it to the blacklist. Each node on the blacklist has an associated counter, which is incremented each time a new alert is presented showing that node performed an attack. Third mechanism is evading attacker via malice-aware routing. In this technique, once attackers have been identified with blacklists, nodes can actively avoid them when routing KBR requests.

6. ANALYSIS AND DISCUSSION

In this section, all the attacks and its defense techniques are analyzed respectively in the above mentioned order.

6.1 After the analysis it shows that the above technique provides a build-in protection mechanism to counter DDoS attacks i.e. the flooding traffic is significantly strangled and most of them is dropped in a close proximity to their sources. The resource isolation of the tIP router protects the normal traffic from flooding traffic, which belongs to different transport protocol. The tIP router assures for high-tiered TCP sessions, gives better service, yield better performance in terms of loss rate, end-to-end delay and effective throughput than low-tired TCP sessions. It achieves better service quality for high-tired services and improves the performance of BE TCP sessions [7].

6.2 The technique used is only useful for packet filtering. It defends against the Internet DDoS attacks. It control on the attack graph information obtained from IP-traceback, use this information to filter out the packets which are more probably come from attackers. This scheme alone is not sufficient for maintaining normal quality of service during heavy attacks. The combination of other DDoS defense technique with this will be more effective [8].

6.3 Usually, the edge routers form a boundary between the ISP network and rest of network. It is known as ISP perimeter. This parameter can be used as defense barrier against network interferences. Suggested two methods alleviate DDoS attacks by blocking the flooding sources, while allowing most legitimate traffic to reach the destination [9].

6.4 The suggested method in [10], is based on a probabilistic packet marking. It is used to locate and eliminate possible attackers instead of dealing with the issue of detecting a DDoS attack. It determines the local traffic rate of each router in the attack graph, by improving the above method. It eliminates the local traffic and accurately determines the local traffic rate of every participating router in the attack graph.

6.5 In [11], attacks are efficiently detects, marks, and redirects traffic away from the traffic using existence proofs, blacklists and malice-aware routing. These techniques are easily applied to and highly effective on real applications just like cooperative file system (CFS). Measurements on CFS perform at least as well as other proposed approaches in detection and recovery. The Eclipse attack and corrupting the lower levels of a victim's routing table are also successfully defended. The weaknesses of all structured overlay protocols are common.

7. CONCLUSION & FUTURE SCOPE

In this paper, different security aspects are studied. These techniques are essential for distributed environment. In this paper various types of attack and techniques are discussed to sustain and block the attack based on the presently existing literature. However, after explicitly reviewed, it is concluding that making a system dynamic and adaptive is the futuristic era and it is the most challenging task.

8. REFERENCES

[1] Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, John L. Schultz, Jonathan Stanton and Gene Tsudik, "Secure Group Communication Using Robust Contributory Key Agreement", IEEE Transactions On Parallel And Distributed Systems, Vol. 15, No. 5, pp. 468-480, May 2004.

[2] Ehab S. Al-Shaer and Hazem H. Hamed, "Modeling and Management of Firewall Policies", eTransactions on Network and Service Management, pp. 2-10, Second Quarter 2004.

[3] Subramanian Lakshmanan, Mustaque Ahamad, and H. Venkateswaran, "Responsive Security for Stored Data", IEEE Transactions On Parallel And Distributed Systems, Vol. 14, No. 9, pp. 818-828, September 2003.

[4] Li Xiao, Zhichen Xu and Xiaodong Zhang, "Low-Cost and Reliable Mutual Anonymity Protocols in Peer-to-Peer Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 14, No. 9, pp. 829-840, September 2003.

[5] Ghassan Misherghi, Lihua Yuan, Zhendong Su, Chen-Nee Chuah and Hao Chen, "A general Framework for Benchmarking Firewall Optimization Techniques", IEEE Transactions On Network and Service Management, Vol. 5, No. 4, pp. 227-238, Dec 2008.

[6] Dhruv Chopra, Henning Schulzrinne, Enrico Marocco, and Emil Ivov, "Peer-to-Peer Overlays for Real-Time Communication: Security Issues and Solutions", IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, First Quarter, pp. 4-12, 2009.

[7] Haining Wang and Kang G. Shin, "Transport-Aware IP Routers: A Built-In Protection Mechanism to Counter DDoS Attacks", IEEE Transactions On Parallel And Distributed Systems, Vol. 14, No. 9, pp. 873-884, September 2003.

[8] Minho Sung and Jun Xu, "IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks", IEEE Transactions On Parallel And Distributed Systems, Vol. 14, No. 9, pp. 861-872, September 2003.

[9] Shigang Chen and Qingguo Song, "Perimeter-Based Defense against High Bandwidth DDoS Attacks", IEEE Transactions On Parallel And Distributed Systems, Vol. 16, No. 6, pp. 526-537, June 2005.

[10] Terence K.T. Law, John C.S. Lui and David K.Y. Yau, "You Can Run, But You Can't Hide: An Effective Statistical Methodology to Trace Back DdoS Attackers", IEEE Transactions On Parallel And Distributed Systems, Vol. 16, No. 9, pp. 799-813, September 2005.

[11] Krishna P.N. Puttaswamy, Haitao Zheng, and Ben Y. Zhao, "Securing Structured Overlays against Identity Attacks", IEEE Transactions On Parallel And Distributed Systems, Vol. 20, No. 10, pp. 1487-1498. October 2009.

Authors

Varsha Tondre, received the degree of M.Sc. in computer science in 1997 from S.R.T.M. University, Nanded. Presently, working as Co-ordinator, Department of Computer Science, in the Brijlal Biyani Science College, Amravati and having 10 years of teaching experience. Her area of research is Distributed Computer Network and security and doing her Ph.D. in Dynamic Resource Management in Distributed Systems. Number of papers on her credits at National & International level journals and conferences.

Dr V M Thakare is Professor and Head of PG department of computer Science and Engg in SGB Amravati University Amravati, Maharastra (India). He has completed his master's degree ME in Advance Electronics in year 1989 and then completed Ph.D in the subject computer Science/Engg in the Area of Robotics and Artificial Intelligence. Currently he is doing research in area of wireless computing, mobile computing, Information Technology and related fields. He is recognized supervisor for computer science and computer engineering in SGB Amravati University and also in other universities including international universities. He has also received national level Award for excellent paper. More than 10 candidates are working for Ph.D. under his supervision. He has published and presented more than 115 papers at National and International level. He has also worked on various national level bodies like AICTE/UGC and also worked on various bodies of other universities. He is presently member of BOS, RRC, BUTR of SGB Amravati university and also chairman and Member of various committees of SGB Amravati university.

He has worked as a head of the department of SGB Amravati University for more than 10 years and remained instrumental to start many new courses in the region like MSc Computer and MCA. Currently the department has started the 1 year PG Diploma course in e-learning and m-learning under the able guidance of Hon'ble vice-chancellor Dr Kamal Singh

Dr. Swati Sherekar is Asst. Professor, PG department of computer Science and Engg in SGB Amravati University Amravati, Maharastra (India). She has received the degree of M.Sc. in computer science in 1994 from SGB Amravati University, Amravati, and then completed Ph.D in the subject computer Science in the area of Digital Watermarking for multimedia authentication. She is having 15 years of teaching experience. Her area of research is Network security, Image Processing. Number of papers on her credits at National & International level journals and conferences. She served as Reviewer for number of International & National Conferences and as chairman/member of many expert/technical committee at state and national level.

Dr. Rajiv Dharaskar is presently working as Professor at PG Department of Computer Science and Engineering, GH Raisoni College of Engineering, Nagpur. He is **Ph.D**. in Computer Science & Engineering in the Faculty of Engineering & Technology, M.Tech. in Computers, P.G. Dip., M.Phil., and M.Sc. He is having 24 years of teaching and 18 years of R&D experience in the field of Computers & IT. He is approved PhD guide for Computer Engineering and Science for Nagpur and Amravati University and 22 research scholars are perusing Ph.D. degree under his guidance. He is an author of number books on Programming Languages.

He has been actively involved in the research on Mobile Computing, Mobile Forensic Security, Multimedia, Software Engineering, Web Technology, HCI, e-Commerce, E-Learning, NLP, Soft Computing, Networking and Wireless Technologies etc. He has authored 22 Journal Papers and 85 research papers at various International and National Conferences. He has been invited as a Keynote or Invited Speaker for 26 International & National Conferences. He is on editorial board of 9 International Journals and worked as a Reviewer for 12 International Conferences and number of national conferences. He has worked as Technical Committee Member for 12 International conferences & number of National Conferences.