DEPLOYMENT ISSUES OF SBGP, SOBGP AND PSBGP: A COMPARATIVE ANALYSIS

Naasir Kamaal Khan[1], Gulabchand K. Gupta[2], Z.A. Usmani[3]
[1,2]*Information Tech. Deptt., Institute of Engineering, J.J.T University, Rajasthan, India.*
[3]*Computer Engg. Deptt., M.H.S.S College of Engineering, Mumbai University, India.*

ABSTRACT

Border Gateway Protocol (BGP) is the protocol backing the core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). Point of concern in BGP is its lack of effective security measures which makes Internet vulnerable to different forms of attacks. Many solutions have been proposed till date to combat BGP security issues but not a single one is deployable in practical scenario. Any security proposal with optimal solution should offer adequate security functions, performance overhead and deployment cost. This paper critically analyzes the deployment issues of best three proposals considering trade-off between security functions and performance overhead.

KEYWORDS: *BGP, secure BGP, secure origin BGP, pretty secure BGP, inter domain routing, ASes.*

I. INTRODUCTION

The Border Gateway Protocol (BGP) [1], has provided interdomain routing services for the Internet's disparate component networks since the late 1980's [2]. Given the central role of routing in the operation of the Internet, BGP is one of the critical protocols that provide security and stability to the Internet [3].

BGP's underlying distributed distance vector computations rely heavily on informal trust models associated with information propagation to produce reliable and correct results. It can be likened to a hearsay network information is flooded across a network as a series of point-to-point exchanges, with the information being incrementally modified each time it is exchanged between BGP speakers. The design of BGP was undertaken in the relatively homogeneous and mutually trusting environment of the early Internet.

Today's inter-domain routing environment remains a major area of vulnerability [3]. BGP's mutual trust model involves no explicit presentation of credentials, no propagation of instruments of authority, nor any reliable means of verifying the authenticity of the information being propagated through the routing system. Hostile actors can attack the network by exploiting this trust model in inter-domain routing to their own ends. Current research on BGP is predominately focused on two major themes; scaling, and resistance to subversion of integrity [4].

A key question is whether further information can be added into the inter-domain routing environment such that attempts to pervert remove or withhold routing information may be readily and reliably detected. Any proposed scheme(s) must also be evaluated for their impact on the scaling properties of BGP [5]. In second section of the paper BGP Architecture is discussed in detail with its vulnerability against associated attack vectors and resulting consequences of such attacks. In third section three best proposals are discussed including their architecture, functionality and mechanism. In forth section a rigorous comparative analysis has been done with deployment issues of each solution. In fifth section conclusion has been obtained with some open questions for further research.

II. THE BGP ARCHITECTURE

The Internet's routing system is a structured two-level hierarchy [6]. At the bottom level we have routing elements grouped into Autonomous Systems (ASes) [7]. Each AS represents a collection of

routing elements sharing a common administrative context. Where a BGP speaker is presented with multiple paths to the same address prefix from a number of peers, the BGP speaker selects the "best" path to use by minimizing a distance metric across all the possible paths as shown in figure 1. The distance metric used by BGP speakers is the AS Path length. This BGP-selected route object is used to populate the local forwarding table. The BGP speaker then assembles a new route object by taking the locally selected route object, attaching locally significant attributes and adding its own AS value to the route objects AS path vector. This route object is then announced to all BGP peers.

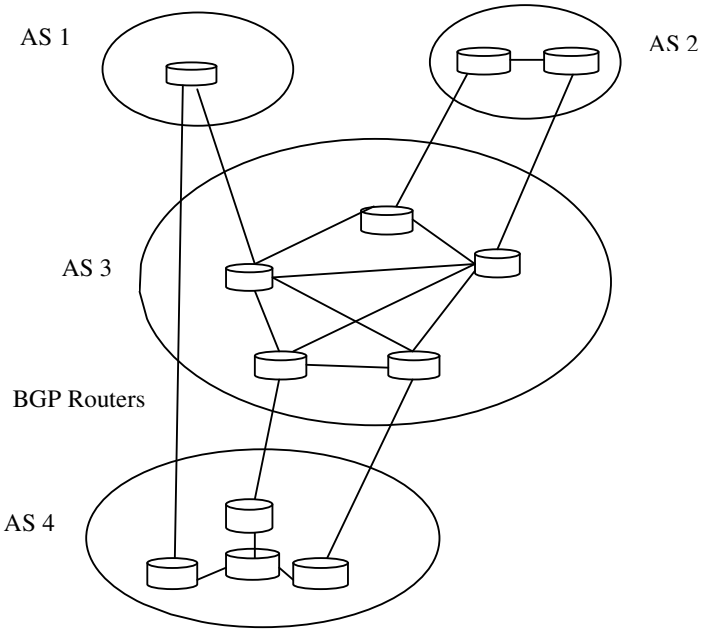

Figure1 BGP Architecture

One approach is to provide taxonomy for threats in routing in general, and BGP in particular, is to view a BGP peer session as a conversation between two BGP speakers and pose a number of questions relating to this conversation which includes the manner in which the BGP session between the BGP speakers is secured, verifying the identity of the other party, verifying the authenticity of the routing information, verifying that the routing information actually represents the state of the forwarding system i.e. Is the information still valid?

2.1 Attack Vectors and Securing BGP session

A BGP session between two routers is assumed to have some level of integrity at the session transport level. BGP assumes that the messages sent by one party are precisely the same messages as received by the other party, and assumes that the messages have not been altered, reordered, have spurious messaged added into the stream or have messages removed from the conversation stream in any way. As with any long-held TCP session, the BGP peer session is vulnerable to eavesdropping, session reset, session capture, message alternation and denial of service attacks via conventional TCP attack vectors.

Attack Vectors are eavesdropping, session hijacking, MITM, modification and DOS at TCP/IP level. Validation of members and IP spoofing are common attacks at identification level. Path Validation, prefix hijacking & impersonation etc are vulnerable at information level. Masquerading is a common attack at route validation level.

Route Flap Damping (RFD) [9], [10] is a widespread defensive BGP configuration that monitors the frequency of BGP updates for a given prefix from each peer, and if the update rate exceeds a locally set threshold the peer's advertisement of this prefix will be locally suppressed for a damping interval. The replay of updates could be used to trigger an RFD response in the remote BGP speaker [11]. If a route is fully dampened through RFD, updates for this prefix will not be advertised by the BGP speaker for a damping interval, possibly causing a route to be disrupted within that time frame.

Another form of threat is by withholding traffic. BGP uses KEEPALIVE timers to determine remote end "LIVENESS". By intercepting and withholding all messages for the hold down timer interval, a third party can force the BGP session to be terminated and reset. This causes the entire route set to be re-advertised upon session resumption so that repeated attacks of this form can be an effective form of denial of service for BGP. It is also possible to undertake a saturation attack on a BGP speaker by sending it a rapid stream of invalid TCP packets. In this case the processing capability of the BGP speaker is put under pressure, and the objective of the attack is to overwhelm the BGP speaker and cause the BGP session to fail and be reset.

2.2 The Consequences of Attacks

The ability to alter the routing system provides a broad array of potential consequences [6]. The consequences fall into a number of broad categories which comprises of the ability to eavesdrop, Denial of service, the potential to masquerade, the ability to steal addresses and obscure identity [12], MITM, session hijacking, IP spoofing and prefix hijacking.

III. BGP SECURITY PROPOSALS

The vulnerabilities of BGP arise from four fundamental weaknesses in the BGP and the inter-domain routing environment [6]. These are inability to protect integrity, lack of authenticity verification for an address prefix, inability to verify the authenticity of BGP UPDATE message and no mechanism to verify that the local cache RIB information. The major contribution to this area of study is the secure BGP (sBGP) proposal [13], which is the most complete contribution to date. However, the assumptions relating to the environment in which sBGP must operate, particularly in terms the performance capability of routing systems appear to be beyond the capabilities of routers used in today's Internet [14]. A refinement of this approach, soBGP [15], is an attempt to strike a pragmatic balance between the security processing overhead and the capabilities of deployed routing systems and security infrastructure, where the requirements for AS Path verification are relaxed and the nature of the related Public Key Infrastructure (PKI) is altered to remove the requirement for a strict hierarchical address PKI that precisely mirrors the address distribution framework. Another refinement of the sBGP model, psBGP [16], represents a similar effort at crafting a compromise between security and deployed capability through the crafting of a trust rating for assertions based on assessment of confidence in corroborating material.

3.1 Secure BGP

Secure BGP (sBGP) [13], represents one of the major contributions to the study of inter-domain routing security, and offers a relatively complete approach to securing the BGP protocol by placing digital signatures over the address and AS Path information contained in routing advertisements and defining an associated PKI for validation of these signatures. sBGP defines the "correct" operation of a BGP speaker in terms of a set of constraints placed on individual protocol messages, including ensuring that all protocol UPDATE messages have not been altered in transit between the BGP peers, that the UPDATE messages were sent by the indicated peer, the UPDATE messages contain more recent information than has been previously sent to this BGP speaker from the peer, the UPDATE was intended to be received by this BGP speaker, and that the peer is authorized to advertise information on behalf of the peer Autonomous System. In addition, for every prefix and its originating AS, the prefix must be a validly allocated prefix, and the prefix's "right-of-use" holder must have authorized the advertisement of the prefix and must have authorized the originating AS to advertise the prefix. The basic security framework proposed in sBGP is that of digital signatures, X.509 certificates and PKIs to enable BGP speakers to verify the identities and authorization of other BGP speakers, AS administrators and address prefix owners. The verification framework for sBGP requires a PKI for address allocation, where every address assignment is reflected in an issued certificate [17]. This PKI provides a means of verification of a "right-of-use" of an address. A second PKI maps the assignment of ASes, where an AS number assignment is reflected in an issued certificate, and the association between an AS number and a BGP speaking router is reflected in a subordinate certificate. In addition, sBGP proposes the use of IPSEC to secure the inter-router communication paths. sBGP also proposes the use of attestations. The address and attestations, allow a BGP speaker to verify the

origination of a route advertisement and verify that the AS path as specified in the BGP UPDATE is the path taken by the routing UPDATE message via the sequence of nested route attestations. Inter-operation and information exchange between sBGP elements is shown in Figure 2. sBGP proposes to distribute the address attestations and the set of certificates that compose the two PKIs via conventional distribution mechanisms outside of BGP messages. For Route Attestations it is necessary to pass these attestations via path attributes of the BGP UPDATE message, as an additional attribute of the UPDATE message. There is a number of significant issues that have been identified with sBGP including the computation burden for signature generation and validation, the increased load in BGP session restart, the issue of piecemeal deployment and the completeness of route attestations, and the requirement that the BGP UPDATE message has to traverse the same AS sequence as that contained in the UPDATE message [14], [18], [19].

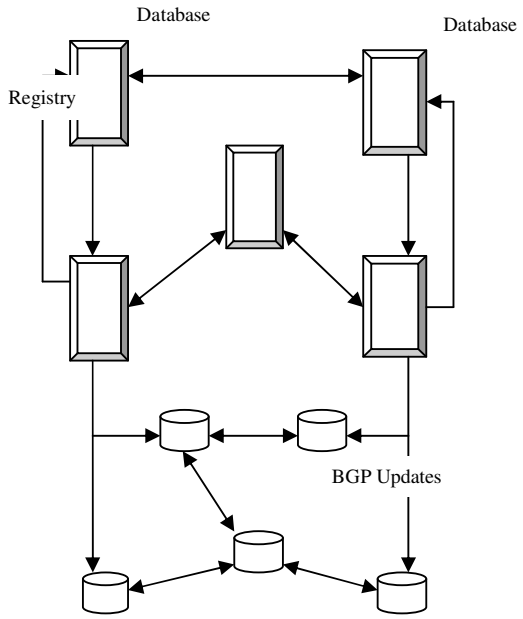

Figure 2 sBGP Mechanism

3.2 Secure Origin BGP

Secure Origin BGP (soBGP) [15] is a response to some of the significant issues that have been raised with the sBGP approach, particularly relating to the update processing load when validating the chain of router attestations and the potential overhead of signing every advertised UPDATE with a locally generated router attestation [20]. The validation questions posed by soBGP also includes the notion of an explicit authorization from the address holder to the originating AS to advertise the prefix into the routing system. The AS path validation is quite different from sBGP however, in that soBGP attempts to validate that the AS path, as presented in the UPDATE message, represents a feasible inter-AS path from the BGP speaker to the destination AS. This feasibility test is a weaker validation condition than validating that the UPDATE message actually traversed the AS path described in the message.

soBGP targets the need to verify the validity of an advertised prefix. It verifies a peer which is advertising a prefix that has at least one valid path to the destination. The best feature of soBGP is that it is incrementally deployable and allows deployment flexibility (on-box or off-box encryption), in its working, BGP verifies the route of originator and its authorization. New BGP message is used to carry security information and it has fixed additional scalability requirements. It uses web of trust model to validate certificate.

soBGP uses the concept of an ASPolicyCert as the foundation for constructing the data for testing the feasibility of a given AS Path. An ASPolicyCert contains a list of the AS's local peer ASes, signed by the AS's private key. AS peer is considered valid if both ASes list each other in their respective ASPolicyCerts. The overall approach proposed in soBGP represents a different set of design trade-offs to sBGP, where the amount of validated material in a BGP UPDATE message is reduced. This

can reduce the processing overhead for validation of UPDATE messages. Also it optimizes memory and encourages distributed processing.
The avoidance of a hierarchical PKI for the validation of AuthCerts and EntityCerts could be considered a weakness in this approach, as the derivation of authority to speak on addresses is very unclear in this model.

3.3 Pretty Secure BGP

Pretty Secure BGP (psBGP) [16] puts forward the proposition that the proposals relating to the authentication of the use of an address in a routing context must either rely on the use of signed attestations that need to be validated in the context of a PKI, or rely on the authenticity of information contained in Internet Routing Registries. The weakness of routing registries is that the commonly used access controls to the registry are insufficient to validate the accuracy or the current authenticity of the information that is represented as being contained in a route registry object. The information may have been accurate at the time the information was entered into the registry, but this may no longer be the case at the time the information is accessed by a relying party. The psBGP approach is also motivated by the proponent's opinion that a PKI could not be constructed in a deterministic manner because of the indeterminate nature of some forms of address allocations. This leads to the assertion that any approach that relies on trusted sources of comprehensive information about prefix assignments and the identity of current right-of-use holders of address space is not a feasible proposition. Accordingly, psBGP rejects the notion of a hierarchical PKI that can be used to validate assertions about addresses and their use. Interestingly, although psBGP rejects the notion of a hierarchical address PKI, psBGP assumes the existence of a centralized trust model for AS numbers and the existence of a hierarchical PKI that allows public keys to be associated with AS numbers in a manner that can be validated in the context of this PKI. This exposes a basic inconsistency in the assumptions that lie behind psBGP, namely that a hierarchical PKI for ASes aligned to the AS distribution framework is assumed to be feasible, but a comparable PKI for addresses is not. Given that the same distribution framework has been used for both resources in the context of the Internet, it is unclear why this distinction between ASes and addresses is necessary or even appropriate. psBGP uses a rating mechanism similar to that used by PGP [21], but in this case the rating is used for prefix origination. An AS asserts the prefix it originates and also may list the prefixes originated by it's AS peers in signed attestation. The ability of an AS to sign an attestation about prefixes originated by a neighbor AS allows a psBGP speaker to infer AS neighbor relationship from such assertions, allowing the local BGP speaker to construct a local model of inter-AS topology in a fashion analogous to soBGP. One of the critical differences between psBGP and soBGP is the explicit inclusion of the "strict" AS Path validation test, namely that it is a goal of psBGP to allow a BGP speaker to verify that the BGP UPDATE message traversed the same sequence of ASes as is asserted in the AS Path of the UPDATE message. The AS path validation function relies on a sequence of nested digital signatures of each of the ASes in the AS Path for trusted validation, using a similar approach to sBGP. psBGP allows for partial path signatures to exist, mapping the validation outcome to a confidence level rather than a more basic sBGP model of accepting an AS path only if the AS Path in the BGP UPDATE message is completely verifiable. The essential approach of psBGP is the use of a reputation scheme in place of a hierarchical address PKI, but the value of this contribution is based on accepting the underlying premise that a hierarchical PKI for addresses is infeasible. It is also noted that the basis of accepting inter-AS ratings in order to construct a local trust value is based on accepting the validity of an AS trust rating, which, in turn, is predicated upon the integrity of the AS hierarchical PKI. psBGP appears to be needlessly complex and bears much of the characteristics of making a particular solution fit the problem, rather than attempting to craft a solution within the bounds of the problem space. The use of inter-AS cross certification with prefix assertion lists introduces considerable complexity in both the treatment of confidence in the assertions and in the resulting assessment of the reliability of the verification of the outcome. psBGP does not consider the alternate case where the trust model relating to addresses is based on a hierarchical PKI that mirrors the address distribution framework. In such a case the calculation of confidence levels would be largely unnecessary.

The major contribution of psBGP relates to the case of partial deployment of a security solution in relation to AS Path validation, where the calculation of a confidence rating in the face of partial security information may be of some utility.

IV. RESULTS AND DISCUSSION

The proposal having the most support from the community is the S-BGP architecture, which employs three security mechanisms, Public Key Infrastructure (PKI) to support the authentication of ownership (secure origin), Digital signatures covering the routing information (AS path validation), IPsec to provide data and partial sequence integrity. In sBGP & soBGP a public key certificate is issued to each BGP speaker whereas psBGP employs common public key certificate for all speakers within one AS resulting requirement of fewer BGP speaker certificates [16].

4.1 Comparative Analysis

Comparative analysis has been done in table 1 based on trust model, topological authentication, path authentication, and origin authentication. It has been observed that origin authentication is strong in sBGP & soBGP whereas path authentication is strong in sBGP and psBGP, although psBGP uses centralized trust model but it is weaker solution than sBGP.

Table 1: Comparative Analysis

Proposal	Trust Model	Topo. Auth	Path. Auth	Origin Auth
sBGP	Centralized	Strong	Strong	Strong
soBGP	Web-of-Trust	Strong	None	Strong
psBGP	Centralized	Weak	Strong	Weak

4.2 Deployment Issues

Deploying S-BGP raises a number of other issues like Adoption of S-BGP by several groups, S-BGP's interaction with other exterior and interior routing, BGP-4 to S-BGP transition. The route attestation path attribute is optional for both external and internal BGP exchanges. This allows extensive regression testing before deploying S-BGP on production equipment. Security Mechanism employed by S-BGP is Public Key Infrastructure (PKI) to support the authentication of ownership (secure origin) Digital signatures covering the routing information (AS path validation) and IPsec to provide data and partial sequence integrity. Deployment of soBGP is done by exchanging certificates at all BGP peering points or AS edges, it processes the certification and build the required soBGP tables at each BGP speaker.

Table 2: Deployment Issues

Proposal	Type	Reference Implementation	Deployed
sBGP	Crypto	Yes	No
soBGP	Anomaly	No	No
psBGP	Crypto	No	No

V. CONCLUSION

BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule sets. For this reason, it is more appropriately termed a reachability protocol rather than routing protocol. Though all of the above solution have their own impact to combat BGP attacks but still some questions are unanswered like, how many AS must implement secure routing, what kind of policies are most suitable for AS to secure BGP architecture globally looking to its tremendous expansion and what should be priorities in securing AS in order to establish highest number of secure routes. sBGP is the best solution among all of them but problems associated with its deployment are unsolved. The most obvious negligence in today's scenario is PKI for addresses and ASes that would allow anyone to verify a digital attestation.

REFERENCES

[1] Y. Rekhter, T. Li, S. Hares. "A border gateway protocol 4 (BGP- 4)" RFC 4271 (Draft Standard), Internet Engineering Task Force, Jan. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4271.txt

[2] Y. Rekhter, "Experience with the BGP protocol," RFC 1266 (Informational), Internet Engineering Task Force, Oct. 1991. [Online]. Available: http://www.ietf.org/rfc/rfc1266.txt
[3] Office of the President of the United States, "Priority II: A national cyberspace security threat and vulnerability reduction program," 2004. [Online]. Available: http://www.us-cert.gov/reading_room/cyberspace_ strategy.pdf.
[4] N. Feamster, H. Balakrishnan, and J. Rexford, "Some Foundational Problems in Interdomain Routing," in *3rd ACM SIGCOMM Workshop Hot Topics Netw. (HotNets)*, San Diego, CA, Nov. 2004.
[5] M. Nicholes and B. Mukherjee, "A survey of security techniques for the border gateway protocol (BGP)," Commun. Surveys and Tuts, IEEE, vol. 11, no. 1, pp. 52–65, Quarter 2009.
[6] B. Donnet and T. Friedman, "Internet topology discovery: a survey," Commun. Surveys Tuts, IEEE, vol. 9, no. 4, pp. 56–69, Quarter 2007.
[7] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an autonomous system (AS)," RFC 1930 (Best Current Practice), Internet Engineering Task Force, Mar. 1996. [Online]. Available: http://www.ietf.org/rfc/rfc1930.txt
[8] A. Ramaiah, R. Stewart, and M. Dalal, "Improving TCP's robustness to blind in-window attacks," Nov. 2008. [Online]. Available:http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-1
[9] C. Villamizar, R. Chandra, and R. Govindan, "BGP route flap damping," RFC 2439 (Proposed Standard), Internet Engineering Task Force, Nov. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2439.txt
[10] P. Smith and C. Panigl, "RIPE routing working group recommendations on route-flap damping," ripe-378, May 2006, obsoletes: ripe-229, ripe- 210, ripe-178. [Online]. Available: http://www.ripe.net/docs/ripe-378.html
[11] K. Sriram, D. Montgomery, O. Borchert, O. Kim, and D. Kuhn, "Study of BGP peering session attacks and their impacts on routing performance," Sel. Areas Commun., IEEE J., vol. 24, no. 10, pp. 1901–1915, Oct. 2006.
[12] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," SIGCOMM Comput. Commun. Rev., vol. 36, no. 4, pp. 291–302, 2006.
[13] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (SBGP)," Sel. Areas Commun., IEEE J., vol. 18, no. 4, pp. 582–592, Apr. 2000.
[14] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure border gateway protocol (S-BGP) – real world performance and deployment issues," in 7th Annual Netw. Distributed Syst. Security Symp. (NDSS'00), Feb. 2000, pp. 103–116.
[15] R. White, "Securing BGP through secure origin BGP," Internet Protocol J., vol. 6, no. 3, Sept. 2003.
[16] P. v. Oorschot, T. Wan, and E. Kranakis, "On interdomain routing security and pretty secure BGP (psBGP)," ACM Trans. Inf. Syst. Secure., vol. 10, no. 3, p. 11, 2007.
[17] K. Seo, C. Lynn, and S. Kent, "Public-key infrastructure for the secure border gateway protocol (S-BGP)," in *DARPA Inf. Survivability Conf.Exposition II, 2001. DISCEX '01. Proc.*, vol. 1, 2001, pp. 239–253 vol 1.
[18] M. Zhao and D. Nicol, "Evaluating the performance impact of PKI on BGP security," Internet 2 4th Annual PKI R&D Workshop, Apr. 2005. [Online]. Available: http://middleware.internet2.edu/pki05/ proceedings/zhao-sbgp.pdf
[19] M. Zhao, S. Smith, and D. Nicol, "The performance impact of BGP security," Netw., IEEE, vol. 19, no. 6, pp. 42–48, Nov.-Dec. 2005.
[20] S. T. Kent, "Securing the border gateway protocol: A status update," in Seventh IFIP TC-6 TC-11 Conf. Commun. Multimedia Security, Torino, 2003.
[21] P. R. Zimmermann, The official PGP user's guide. Cambridge, MA, USA: MIT Press, 1995.
[22] B. S. LLC, "Secure BGP prototype software," 2003. [Online]. Available: http://www.ir.bbn.com/sbgp/src/S-BGP-1.0.html
[23] J. Ng, "Extensions to BGP to support secure origin BGP (soBGP)," Apr. 2004. [Online]. Available: http://tools.ietf.org/html/draft-ng-sobgp-bgp-extensions-02

Authors Biographies

Naasir Kamaal Khan has received his B.E (Hons.), & M.Tech (IT) in 2002 & 2004 respectively. Presently he is Pursuing Ph.D in Information Technology. Over the span of 8 years of his teaching experience he has Published & Presented Several Research Papers in National & International Conferences, Delivered expert lectures in India & Abroad. He has supervised several student research projects. He is a Life Member of Indian Society of Technical Education (ISTE). His areas of interest are Cryptography & Network Security, Information & System Security and Computer Networks.

Gulabchand K. Gupta has received his M.Sc, Ph.D in Electronics and M. Tech in Computer science and engineering. Presently he is Principal at Western college of commerce and business management, Navi Mumbai and Research Guide at J.J.T University. Over the span of 30 years of his teaching experience he has published and presented several research papers in national and international conferences and journals. He has supervised several Ph.D and M.Tech students for their research work. He is a senior member of computer society of India(CSI). His areas of interest are Computer Networks, Mobile Ad-hoc and sensor Networks, Network Security and Wireless Networks.

Z. A. Usmani has received his B.E in Electronics & M.Tech in Computer Science & Engineering. Presently he is working as an Associate Professor and Head at M.H.S.S College of Engineering, Mumbai University. He has more than 30 years of teaching experience. He has Published & Presented Several Research Papers in National & International Conferences. He has supervised several student research projects. His areas of interest are Computer Networks, Cryptography & Network Security, Mobile Computing and Wireless Networks.