Real-Time Attack Monitoring on Telecom Network Using Open-Source Darknet and Honeypot Setup

L. Sivakamy[1], S. Pradheepkumar[1], A. Sivabalan[1]
and Anand R. Prasad[2]

[1]*NEC Technologies India Private Ltd, India*
[2]*NEC Corporation, Japan*
E-mail: sivakamy.l@india.nec.com; pradheepkumar.s@india.nec.com; sivabalan.arumugam@india.nec.com; anand@bq.jp.nec.com

Received 02 August 2017;
Accepted 18 January 2018

Abstract

The traditional use of darknets is to passively monitor malicious traffic in a network. In this paper, we describe an experimental setup that leverages this property of the darknet in a network monitoring setup coupled with several honeypot servers. The honeypots are configured as a decoy to lure cyber attacks on the network. The cyber-security test-bed thus designed enables us to monitor an end-to-end mobile communication network test-bed [1] and detect attacks on the network in real-time. After successful trial runs, the results and alert incidents show that the cyber-security setup is efficient in detecting malicious activity in the network.

Keywords: Darknet, Alerts, Cybersecurity, Honeypots, Cyber attacks, Network monitoring, Malware detection.

1 Introduction

A darknet is a portion of unallocated Internet Protocol (IP) address space in which no responsive servers typically reside [2]. It is most unlikely that such

Journal of ICT, Vol. 5_2, 187–202.
doi: 10.13052/jicts2245-800X.524

unused IP addresses receive packets on usual Internet usage. So, if one does appear, it is either because of misconfiguration or due to malicious activities such as malware scanning for vulnerable devices. Such scans can be spotted by security administrators, without the need for complicated analysis gear or any false positives. Darknet monitoring requires the setup of servers called Darknet Sensors, which act as sinkholes for all packets addressed to the darknet IP addresses [3].

The Darknet sensors have predominantly been used only for passive network monitoring and alert generation [3–5]. In this paper, we extend the capability of the sensors to conduct deep packet inspection on the captured inbound packets. The analysis pertains to the origin of attacks and the approach of attacks (threat model). In order to detect more types of attacks, honeypots [6] are configured in the same network as the darknet IP addresses. These honeypots act as deception traps that entice attackers to spend time on the services employed. The analysis of the myriad of attacks is vital in discovering vulnerabilities in the network design, strengthening the actual network and inoculating and immunizing the network against possible attacks in future.

To identify possible attacks on the network and generate alerts, rule-based and signature-based detection techniques were used. Signature-based detection works by comparing the logged packet to a list of previously known attack signatures, mostly using string comparison operations. But, this technique is largely ineffective in detecting previously unknown threats, variants of known threats and more importantly, the latest and recently reported threats [7]. The proposed test-bed overcomes this shortcoming by extending the functionality of the darknet sensor server to dynamically detect even the most recent malware signatures from latest online malware/threat databases. This paper explains the design, development, and implementation of a test-bed that consists of a sensor server that monitors all the traffic destined to honeypot servers and identifies real-time threats to the monitored network(s). As a practical use-case in this paper, the test-bed is extended to monitor mobile communication network [1] to identify real-time threats and potential attacks.

The organization of the paper is as follows. In Section 2, we give an overview of the previous work which have shown the feasibility of using darknets for monitoring networks. In Section 3, we discuss the test-bed architecture. We also explain the overall implementation of the test-bed in Section 4. The results are discussed in Section 5. Conclusion and future work are elicited in Section 6.

2 Related Work

This section elicits the related work carried out around the world with respect to darknets and monitoring live networks.

Cooke, Baily, Watson and Jahanian proposed a distributed global Internet monitoring system whose goal was to track measure and characterize threats. They introduced the concept of Internet Motion Sensor (IMS) that employs a distributed infrastructure that makes use of sensors that actively categorize IP addresses. The active component in the blackhole sensors only responds to Transmission Control Protocol (TCP) connection requests. The paper also discusses a technical study of various internet threat monitoring architectures and the advantages of employing sensor-based alert systems [8].

Yegneshwaran, Barford and Plonka discussed the prospects of monitoring both used and unused addresses in order to improve the effectiveness and perspective of Intrusion Detection Systems (IDSs). They propose architecture to create sinkholes (iSink) for packets addressed to the target addresses. Unused addresses tend to respond easily to packets and the information about incoming packets are logged in the sinkhole. This paves way for passive packet capture and analysis [3].

Moore et al. discussed the prevalence of Denial of Service (DoS) attacks to quantitatively assess the nature of such threats in the long run. They analysed several threats including IP Spoofing and Backscatter worms using an experimental platform of few /8 addresses. They had captured around 12,805 attacks over the course of one week. They presented a new technique called "backscatter analysis" to estimate and quantify DoS attacks directed at specific internet services [4].

Yegneshwaran et al. discussed the concept of "background radiation" that reflects and reveals incessant internet activity, either malicious or benign. They deployed sinkholes on the intra-campus routers that filter all the traffic for active trace collection. They analyse the activity across their campus and visualize the traffic using line graphs and bar charts [3].

Moore et al. presented a technical report titled "Network Telescope" that monitors over 160,000 addresses for backscatters and worms. It was a project funded by the Cooperative Association for Internet Data Analysis (CAIDA) in the U.S [5].

Oberhide, Karir, Meo characterized the behaviour of dark Domain Name Service (DNS) – the DNS queries that are associated with darknet addresses. They acquired two class B subnets and delegated DNS authority for these to the collector. Initially, they passively recorded all incoming traffic in the collector.

Later, they extended the framework by replying with a NXDOMAIN (non-existence) error code. They analysed the unusual distribution in the number of queries, target IP addresses and the query sources [9].

Bailey, Cooke, Jahanian Myrick and Sinha published a paper to describe and analyse the issues associated with deploying large-scale darknets. They evaluated the configuration and placement of darknets along with resource provisioning. They demonstrated that using a darknet as a monitoring tool is a productive and significant method to gain visibility into network threats and the state of local networks and the global Internet as well [10].

Suzuki and Inoue proposed a practical alert-based system on darknet monitoring for live networks called Direct Alert Environment for Darknet And Livenet Unified Security (DAEDALUS), which monitors malicious packets transmitted internally based on distributed darknets implemented in multiple organizations. The architecture consisted of a centralised analysis center that was used to alert to the respective organizations in case of any security violations [2].

Each of these focuses on capturing and logging general malicious activity in the network. Our work focuses on deploying a test-bed to generate alerts based on the most recent malware database and analyse vulnerabilities in the network. As a practical use-case, the paper demonstrates how to extend the darknet set-up to monitor the mobile communication network.

3 Architecture

This section describes the architecture of the cyber-security test-bed that is used to identify and log real-time attacks on the network. The test-bed is also used to monitor a mobile communication network and identify real-time attacks to it. As shown in Figure 1, the test-bed consists of two components - the darknet sensor server and the honeypot server. The sensor server analyses the inbound traffic and relays it to the corresponding honeypot server. The information about the packets and the alerts generated by the setup is accessible by the system administrator for analysis.

The router is configured to re-route all the traffic destined to the darknet IP addresses (referred to as the darknet hereof) to the sensor server, which is designed to capture and log the packet information. Preliminary analysis is done here and reports are generated periodically. The server then forwards the traffic to the respective honeypot server. Figure 2 depicts the architecture of the honeypot server configured with services, which lure attackers to try and exploit the vulnerabilities in them.

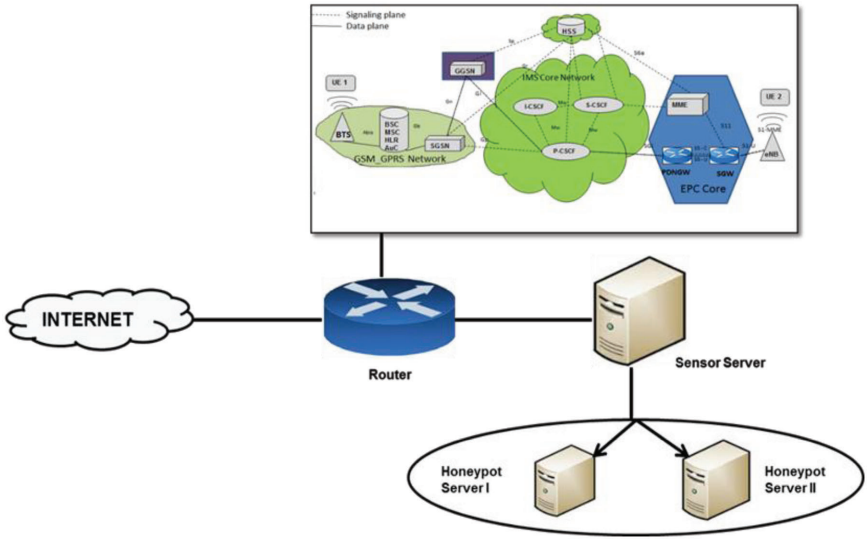

Figure 1 Cyber-security test-bed setup.

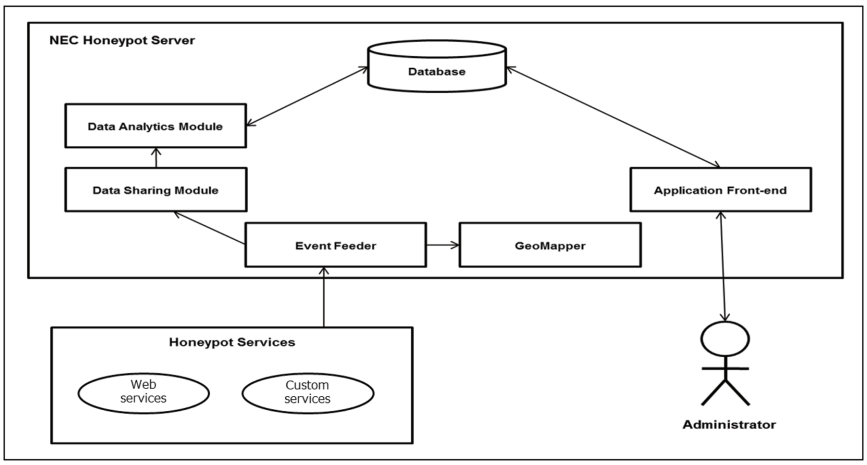

Figure 2 Honeypot server architecture.

Such activities and threats to the system are detected in real-time and reported to the system administrator. The events generated by the honeypot services, deployed in the server, are logged in the attack database. These are used to generate real-time reports and plot the location of the attacker on the world map. Monitoring of a live mobile communication network is then added as a service in the test-bed to identify and report real-time threats to it.

The greatest advantage of using this setup is that no major change is required in the existing network configurations of the organization. The test-bed can also be scaled on-demand.

4 Implementation of the Test-Bed

This section gives a detailed account of the implementation of the cyber-security test-bed. The implementation of the test-bed was carried out in three phases. The first was the design of the sensor server and supporting components. The second was designing and developing the server to generate real-time alerts for potential threats. The last phase was to introduce the cyber-security test-bed on top of the end-to-end mobile communication network [1] to log and monitor threats to it.

4.1 Implementation of the Sensor Server

The setup is designed in such a way that the packets addressed to the darknet are re-routed to the darknet sensor for analysis. Ten unused IP addresses in a /24 network were monitored by this darknet sensor. For this, static routes are pre-set in the router's settings. The sensor is configured with packet analysis tools for deep packet inspection. Once the packets reach the sensor server, they are analysed based on source and destination addresses, ports and protocols.

Snort [11] IDS is implemented in the sensor to give real-time alerts of all malicious packets addressed to the darknet. The packet details are logged into the MySQL [12] database. The IDS was enhanced to analyse packets using a specially designed module that uses the most recent online malware databases and repositories of blacklisted IPs to generate alerts. The sensor then forwards the packets destined to the honeypot to the development server which hosts several services. For this, the darknet sensor server is configured with two Network Interface Cards (NICs)- one to sniff incoming traffic and the other to forward traffic to the honeypots. The honeypot server is designed to aggregate the details of all such attacks and create real-time reports on the web front end and visualize the location of the attacker on the world map.

4.2 Implementation of the Honeypot Server

As discussed in Section 3, the Honeypot server is designed as a trap to entice attackers to try and attack the system. Two honeypot servers are configured with fake web services and protocol emulations in separate Virtual Machines

(VMs) in the same network as that of the darknet. Global IP addresses are assigned to the servers to make them accessible from external networks. This is done to identify the different types of vulnerabilities in the network.

The Honeypot server consists of an Event Feeder that feeds the events generated by the Honeypot Services deployed in it. The Data-Sharing module aggregates the events. This module can be scaled to consolidate events from services deployed across multiple honeypot servers. The events are classified based on pre-defined rules by the Data Analytics module and then stored in the Database. The origins of the attacks are plotted in real-time on the world map by the GeoMapper. A Web Application frontend is designed to facilitate administrative access to the dashboard for real-time management of the deployed services. The web frontend can also be used by administrators to deploy new honeypot services and edit or update the rules based on which the attacks are classified. The frontend is designed using Ruby-on-Rails to create graphs and reports based on protocols, destination, source, ports, signature and priority. The priorities are configured based on exploit-type, endangered resources, and the severity and chronology of the attack. The classification of threats based on priority is a separate work in itself and is out of scope of this paper. In case of high-severity events, the detailed incident report is sent to the administrator.

4.3 Implementation of Mobile Communication Network Monitoring

The traffic destined to the mobile communication network is captured and analysed by the IDS configured in the test-bed. The IDS uses rule-based detection to identify and generate alerts. This way, all traffic reaching the end-to-end mobile communication network [1] is screened by the test-bed to generate real-time alerts.

5 Results

This section explains in detail the results obtained from the deployment of the test-bed. Table 1 gives the distribution of the protocols of packets captured by the set-up.

Figure 3 illustrates the distribution of TCP, UDP, GTP and SCTP packets over time as logged by the test-bed. The figure describes the inflow of packets to the LTE network. The details of the packets were logged by the sensor server and alerts were generated based on pre-defined rules.

Table 1 Protocol Distribution

Protocol	Number of Packets
TCP	759095
UDP	26163
ICMP	5807

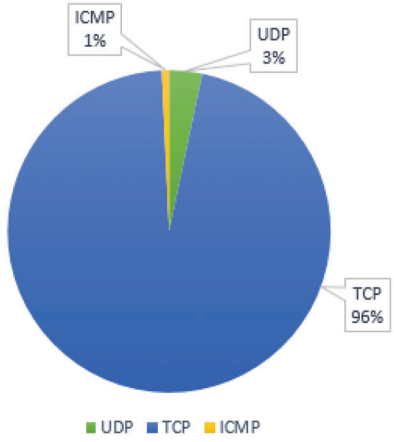

Figure 3 Distribution of packets based on protocol.

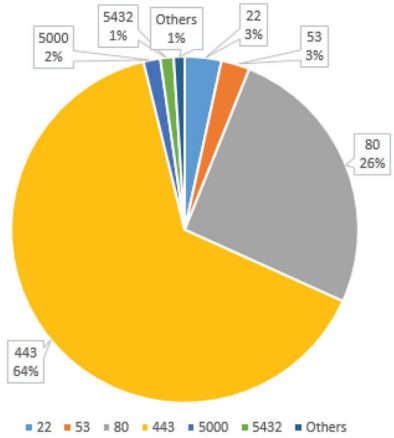

Figure 4 Distribution of packets based on ports.

Figure 4 shows the distribution of packets based on ports. The ports were susceptible to heavy port scanning in periodic short bursts. Most of the activity logged was mapped to IPs in China, USA, Brazil and UK.

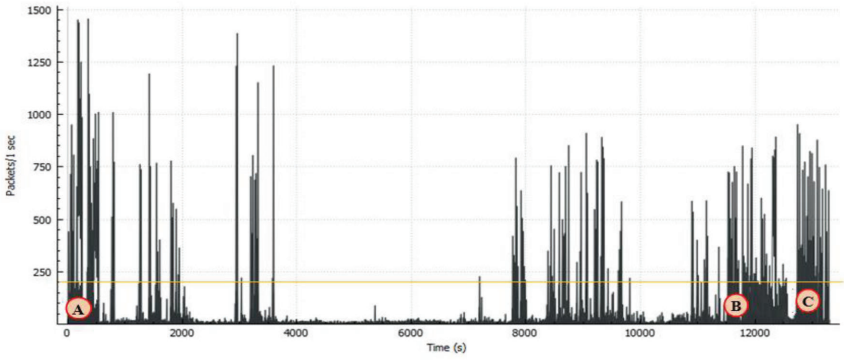

Figure 5 Sample distribution of alerts (in packets per second).

Figure 5 shows the distribution of packets logged by the sensor per second over period of three hours. The sensor server was pre-configured with rules to identify potentially malicious packets. The alerts generated based on the rules were classified as high priority, medium priority and low priority based on the severity of the threat.

The regions encircled in the graph in Figure 5 showed an abnormal upsurge in alert rates. Upon investigation, it was identified that alerts in regions A and C were of medium priority while region B had a high priority alert reported.

All anomalies over a period of one week were aggregated out of which few are listed in Sections 5.1 and 5.2.

5.1 Incidents Related to Port Scanning and SSH Bruteforce Attacks

- **Incident 1:** Our test-bed reported a total of 12532 alerts from a specific IP address in short bursts, spanning a total of three hours. Upon further investigation, it was detected to be an SSH Brute force attack against port 22.
- **Incident 2:** Our test-bed reported a total of 3893 packets from a specific IP address within a span of half an hour. Upon investigation, it was identified as an SSH Brute force attack against port 22.
- **Incident 3:** Our test-bed reported a total of 3291 packets sent to the network by a group of IP addresses listed with the same subnet. Upon further investigation, it was detected to be an SSH Brute force attack against port 22. The attack continued over the span of two days with different IP addresses carrying out the attack.

- **Incident 4:** We detected a total of 616 packets sent to the network by a specific IP address under a span of three minutes. It was confirmed to be an SSH Brute force attack and port scan against port 22.
- **Incident 5:** Our test-bed reported an SSH Brute force attack, port scan and FTP Brute-force attack by a specific IP address in a span of less than three minutes against ports 22 and 443.
- **Incident 6:** Our test-bed reported an SSH Brute force attack and port scan by a specific IP address against ports 21, 22, 80 and 443.

5.2 Incidents Related to Malware

- **Incident 1:** Our test-bed reported multiple alerts from an IP that was flagged as malicious due to several SSH login attempts. The IP address was previously flagged for threats such as *Linux.DownLoader.115, Trojan.DownLoader19.51775 and Linux/Setag.B.Gen trojan.*
- **Incident 2:** Our test-bed reported alerts from a specific IP address at bursts of two minutes with an average of 561 packets per each burst against ports TCP ports 443 and 137. Investigation of the IP address reported that it was infected with malware and was involved in phishing. The malware and Trojan detected was *Win32/DoS.FTP.KillCerb Trojan, Win32/Bagle.AB worm, Win32/Exploit.DCom.BW Trojan, Win32/ Netsky.Q worm, HTML/Exploit.IESlice.AJ Trojan, Perl/DoS.Nertt Trojan and VBS.Psyme.126 and Perl/Shellbot.NAK.Gen Trojan*.
- **Incident 3:** Our test-bed reported alerts from a specific IP address, which upon investigation was reported earlier as malware. The specific threats logged were *Source Code/exploits/ms06-067-keyframe.html - HTML/Shellcode.Gen.*
- **Incident 4:** Our test-bed reported an average of 142 alerts per second by a specific IP address. Investigation of the source IP address reported that it was flagged for propagating malware such as *Troj/SEO-A, Trojan.DownLoader13.6370 and W32/Felix:Process_related!Eldorado.*
- **Incident 5:** Our test-bed reported an average of 732 packets per minute from a specific IP address. Investigation of the IP address reported that the IP it was flagged for threats such as *VBS/Worm and Perl/Exploit.WSFT Trojan*.
- **Incident 6:** Our test-bed reported a high-priority attack from a specific IP address which had been blacklisted earlier for reportedly propagating malware such as *BackDoor.OnionDuke.1 and HTML/Framer Virus.*

6 Conclusion

The proposed cyber-security test-bed leverages darknet and honeypot deployments to actively monitor networks in real-time. The simplicity of the setup lies in the fact that it can be scaled for any type of network, telecom or otherwise. The test-bed monitors malicious packets destined to the deployed services and also monitors traffic within the network itself.

Based on pre-configured rules, the Data Analytics module detects malware infections and other anomalies. All alerts are logged automatically. In case of high severity threats, the administrator is intimated of the situation and an incident report is generated.

The setup also monitors a live end-to-end mobile communication network to detect potential threats and attacks in real-time. Such real-time detection reports become invaluable in securing and inoculating the network from similar attacks.

Another feature of this setup is that multiple honeypot servers, deployed can be connected to the sensor server. It is also well-equipped to handle dynamic up-scaling. In such a case, events from all honeypot deployments can be aggregated and managed by the administrator simultaneously.

Operational results of the test-bed and incidents show that the cyber-security setup was successful in detecting malicious activity such as trojans, backdoors and worms in the network. Going forward, we will develop an intelligent system that automatically detects new attacks and also analyses the strategies and technologies used by the attackers. And more specifically, we will focus more on intrusion detection in the realm of Telecom network-Monitoring-as-a-Service.

References

[1] George, K. J., Sivabalan, A., Prabhu, T., and Prasad, A. R. (2015). "End-to-End Mobile Communication Security Testbed Using Open Source Applications in Virtual Environment." *J. ICT Standardization*, 3(1), 67–90.

[2] Suzuki Mio and Inoue Daisuke, (2017). "DAEDALUS: Practical Alert System Based on Large-scale Darknet Monitoring for Protecting Live Networks", *Journal of the National Institute of Information and Communications Technology*, 58.

[3] Yegneswaran, V., Barford, P., and Plonka, D. (2004). "On the design and use of Internet sinks for network abuse monitoring". In *International*

Workshop on Recent Advances in Intrusion Detection, (pp. 146–165). Springer, Berlin, Heidelberg.

[4] Moore, D., Voelker, G., and Savage, S. (2001). "Inferring Internet Denial of Service Activity", In *10th USENIX Security Symposium*, Washington D.C.

[5] Moore, D., Shannon, C., Voelker, G. M., and Savage, S. (2004). "*Network Telescopes: Technical Report*", Tech. rep., Cooperative Association for Internet Data Analysis (CAIDA), San Diego.

[6] Campbell, R. M., Padayachee, K., and Masombuka, T. (2015). "A survey of honeypot research: Trends and opportunities", In *10th International Conference for Internet Technology and Secured Transactions (ICITST)*.

[7] Scarfone, K., and Mell, P. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Computer Security Resource Center. National Institute of Standards and Technology (800–94). Retrieved 1 January 2010.

[8] Cooke, E., Bailey, M., Watson, D., Jahanian, F., and Nazario, J. (2004). *The Internet motion sensor: A distributed global scoped Internet threat monitoring system*. Technical Report CSE-TR-491-04, University of Michigan, Electrical Engineering and Computer Science.

[9] Oberheide, J., Karir, M., and Mao, Z. M. (2007). Characterizing Dark DNS Behavior. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 140–156). Springer, Berlin, Heidelberg.

[10] Bailey, M., Cooke, E., Jahanian, F., Myrick, A., and Sinha, S. (2006). Practical darknet measurement. In *Information Sciences and Systems, 40th Annual Conference* (pp. 1496–1501). IEEE.

[11] Snort. Available at: https://www.snort.org/

[12] MySQL. Available at: https://www.mysql.com/

[13] Song, D., Malan, R., and Stone, R. (2001). *A snapshot of global Internet worm activity*. Technical report, Arbor Networks.

[14] Wang, Q., Chen, Z., and Chen, C. (2011). Darknet-based inference of internet worm temporal characteristics. *IEEE Transactions on Information Forensics and Security*, 6(4), 1382–1393.

[15] Pang, R., Yegneswaran, V., Barford, P., Paxson, V., and Peterson, L. (2004). Characteristics of internet background radiation. In *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement* (pp. 27–40). ACM.

Biographies

S. Lakshminarayanan received B.E. in Computer Science and Engineering from Rajalakshmi Institute of Technology, India in 2016. She has 20 months of experience in research and development of mobile communication networks and security standardization. At present she works as Member Technical Staff in NEC India Standardization (NIS) Team at NEC Mobile Network Excellence Center (NMEC), NEC Technologies India Pvt Ltd, Chennai. In her current role, she is working on Security aspects of 5G systems and has applied for several patents on the same. Her research interest includes Cyber Security, Telecom Security and Machine Learning.

Pradheepkumar Singaravelu is a Senior Researcher at NEC-India. He has around 10 years of experience in Security domain in different areas such as NFV, IOT, 5G and LTE networks. He represents as one of the security expert for NEC Corporation in global forum such as ETSI-NFV, 3GPP-SA3 and local forum like GISFI, TSDSI, etc. He was the Vice chair of the 5G Working Group in TSDSI. Prior to joining NEC, he worked with Samsung Electronics, India. He worked as a Technical Leader of DTV security platform and Standards group. He has filed several patents which cover a wide range of IoT, NFV and Smart Home Technology. He received Ph.D in Information Technology from Indian Institute of Information Technology, Allahabad. He has published several research papers in reputed international journals and conferences.

S. Arumugam received Ph.D in Electrical Engineering from Indian Institute of Technology Kanpur, India in 2008 and M.Tech degree from Pondicherry University, India, in 2000. He has 14 years of experience in Academic teaching and Research. Presently he works as Assistant General Manager for Research at NEC Mobile Network Excellence Center (NMEC), NEC Technologies India Pvt Ltd, Chennai. Prior joining NECI he was associated with ABB Global Services and Industries Limited, Bangalore as Associate Scientist. He has published more than 25 papers in various International Journals and Conferences and also participated in many National and International Conferences. In his current role, he is representing NEC for Global ICT Standards forum of India (GISFI). His research interest includes Next Generation Wireless Networks.

A. R. Prasad, Dr. & ir., Delft University of Technology, The Netherlands, is Chief Advanced Technologist, Executive Specialist, at NEC Corporation, Japan, where he leads the mobile communications security activity. Anand is the chairman of 3GPP SA3 (mobile communications security standardization group), a member of the governing body of Global ICT Standardisation Forum for India (GISFI), founder chairman of the Security & Privacy working group and a governing council member of Telecom Standards Development Society, India. He was chairman of the Green ICT working group of GISFI. Before joining NEC, Anand led the network security team in DoCoMo Euro-Labs, Munich, Germany, as a manager. He started his career at Uniden Corporation,

Tokyo, Japan, as a researcher developing embedded solutions, such as medium access control (MAC) and automatic repeat request (ARQ) schemes for wireless local area network (WLAN) product, and as project leader of the software modem team. Subsequently, he was a systems architect (as distinguished member of technical staff) for IEEE 802.11 based WLANs (WaveLAN and ORiNOCO) in Lucent Technologies, Nieuwegein, The Netherlands, during which period he was also a voting member of IEEE 802.11. After Lucent, Anand joined Genista Corporation, Tokyo, Japan, as a technical director with focus on perceptual QoS. Anand has provided business and technical consultancy to start-ups, started an offshore development center based on his concept of cost effective outsourcing models and is involved in business development.

Anand has applied for over 50 patents, has published 6 books and authored over 50 peer reviewed papers in international journals and conferences. His latest book is on "Security in Next Generation Mobile Networks: SAE/LTE and WiMAX", published by River Publishers, August 2011. He is a series editor for standardization book series and editor-in-chief of the Journal of ICT Standardisation published by River Publishers, an Associate Editor of IEEK (Institute of Electronics Engineers of Korea) Transactions on Smart Processing & Computing (SPC), advisor to Journal of Cyber Security and Mobility, and chair/committee member of several international activities.

He is a recipient of the 2014 ITU-AJ "Encouragement Award: ICT Accomplishment Field" and the 2012 (ISC)2 Asia Pacific Information Security Leadership Achievements (ISLA) Award as a Senior Information Security Professional. Anand is Certified Information Systems Security Professional (CISSP), Fellow IETE and Senior Member IEEE and a NEC Certified Professional (NCP).