ISO 9001 : 2008

TEC

TELECOMMUNICATION ENGINEERING CENTRE

टी ई सी संचारिका

NEWSLETTER

Vol. 21 NOVEMBER 2017 ISSUE 4

Interaction of ITS-2015 batch Officer Trainees with Hon'ble Minister of Communications

In this Issue

On 4th September, 2017 Officer Trainees of ITS-2015 Batch interacted with Hon'ble Minister of State (IC) Shri Manoj Sinha ji for Communications at Sanchar Bhawan, New Delhi. The Hon'ble Minister congratulated the young ITS Officer Trainees and discussed about future roadmap, role and responsibilities of the ITS officers in the areas of cyber and telecom network security. He also emphasized that the probationers should make constructive use of the experience in other jobs that they have been on before joining the Department of Telecommunications. Smt. Aruna Sundararajan, Secretary (T), while addressing, impressed upon the importance of Bharatnet Project being implemented by BBNL. She also called upon the probationers to explore opportunities for providing affordable broadband services to rural & remote areas.

Smt. Aruna Sundararajan, Secretary (T), Sh. Lav Gupta, Sr. DDG (TEC/NTIPRIT), Sh. R. K. Sharma, DDG (T&A), NTIPRIT, Sh. Saurabh Gupta, DDG (Training), DoT HQ and Sh. H. S. Jakhar, the then Dir (Trg) NTIPRIT were present during the deliberations.

(Sitting from left Shri Vivek Krishna Verma, AD (Trg), NTIPRIT, Shri Manoranjan, ADG (Trg), NTIPRIT, Shri H. S. Jakhar, the then Dir (Trg) NTIPRIT, Shri Saurabh Gupta, DDG (Training), DoT HQ, Shri Lav Gupta, Sr. DDG (TEC/NTIPRIT), Shri Manoj Sinha Hon'ble Minister of Communications, Smt. Aruna Sundararajan, Secretary (T) and Shri R. K. Sharma, DDG (T&A), NTIPRIT, Standing: ITS-2015 batch Officer Trainees)

Security in Telecommunication Networks on Cloud

1.0 Introduction

Cloud computing is being adopted at a rapid rate because it enables its consumers to launch their business quickly and easily without establishing new ICT infrastructure and provide opportunities to provision resources elastically, as required. The distributed and multi-tenant nature of cloud computing, the prevalence of remote access to cloud computing services and the number of entities involved in each process make cloud computing inherently vulnerable to both internal and external security threats. The use of Cloud computing in telecommunications is dependent on the framework of the Internet and suffers from the same vulnerabilities and security threats. While there are several advantages of adopting and migrating to this new technology that makes it an attractive option for applications and telecom service providers, the security threats and vulnerabilities have the potential to seriously challenge its usefulness.

In the present article various security threats and challenges involved in adopting cloud computing in telecommunication networks have been discussed along with certain countermeasures to mitigate them.

The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer is known as Cloud Computing.

2.0 Telecommunication Networks on Cloud

Telecom Service Providers (TSPs) need to innovate to keep up with the competitive pressure of the rapidly changing network and business environment. They need to improve their ability to introduce new revenue-generating services, increase customer satisfaction, and reduce their costs. A key part of this telecom transformation requires service providers to modify their traditional network architectures significantly to improve agility and reduce operating costs. With the success of virtualization and cloud computing in the information technology domain, Telecom Service Providers are now gradually migrating to the use of cloud based resources to reap the same benefits— economies of scale, cost effectiveness, scalability and independence from proprietary appliances. However, using clouds for telecom services is not the same as using them for IT applications; the telecom industry's demanding requirements for high levels of availability and reliability must be met. In addition, telecom operators want to leverage the significant investment they have already made in their existing infrastructure.

2.1 Adoption of Network Function Virtualization (NFV) and Software Defined Networking (SDN)

Typically, telecom software runs on dedicated computer appliances. Launching new network services becomes increasingly difficult as service providers must manage a variety of proprietary pieces of hardware—in addition to the complexity of integrating and deploying these physical devices in a network. To address these challenges, service providers are driving a transformational concept called Network Functions Virtualization (NFV), which moves network functionality to software and leverages commercially available commodity server hardware from the IT sector and teams it with virtualization technology as shown in Figure. 1.

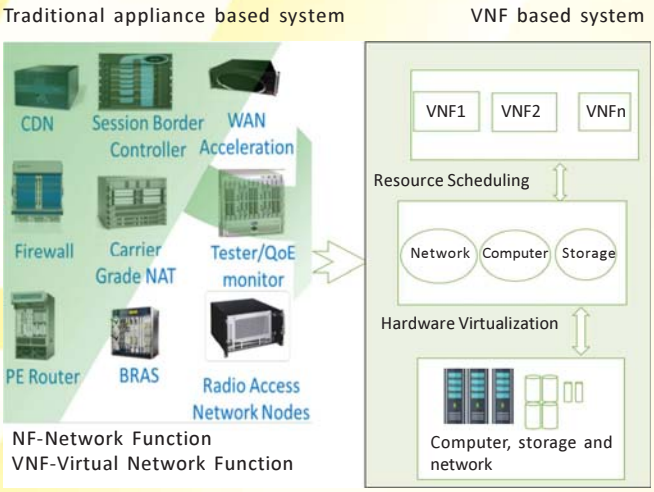

Fig. 1: Evolution from traditional to virtual network function [source: ETSI]

Software-Defined Networking (SDN) refers to the separation of the control plane – where the logic of path computation for complex networks has been implemented – from the data plane, where packets are forwarded based on decisions made in the control plane. SDN increases the utility of NFV.

Using open, standard technologies allows telecom operators to virtualize their proprietary solutions on commercial off the shelf servers. This reduces their time to market because they no longer have to procure individual pieces of hardware for each function in the network. They can just build a rack full of servers & storage and then load the software onto the virtual environment, substantially reducing the amount of

cabling required and leveraging the lower-cost and developer-friendly efficiencies inherent in off-the-shelf equipment.

NFV and SDN adoption is being driven by 5G and IoT because both of these require programmability, flexibility and automation, which are inherent to a software-based solution.

In order to utilise and harness the benefits of Cloud Computing, Government of India has embarked upon an ambitious initiative - "GI Cloud" which has been named as 'MeghRaj'.

2.2 Real Deployment Scenarios

Some real scenarios of cloud deployment already accomplished or under active consideration by the telecom operators worldwide are discussed below.

2.2.1. AT&T has started deploying small cells using C-RAN (Cloud Radio Access Network) architecture in San Francisco. That deployment is being replicated in other cities, enabling the operator to densify its network and lay the groundwork for 5G. In C-RAN architecture, real time(RT) functions are deployed at the antenna site to manage air interface resources, while non-real-time (NRT) control functions are hosted centrally to coordinate transmissions across the coverage area. In 5G, this is being formalized with the central unit (CU) and distributed unit (DU) functional split. This functional architecture is now native to the 3GPP specification. By introducing Cloud RAN architectures, operators will be able to meet these accelerating demands in terms of coverage, capacity, latency, traffic volumes and data rates through the use of Network Functions Virtualization techniques and data center processing capabilities in their networks. It allows for resource pooling, scalability, layer interworking and spectral efficiency.

2.2.2. Softbank, Japan has deployed virtual Mobility Management Entity (vMME) in its network. The deployment represents a complete Network Functions Virtualization (NFV) solution, which operates on commercial off-the-shelf hardware and coexists with native MME to extend the pool. By adding a virtualized environment to its native network, SoftBank can scale its network capability, flexibility and manageability. With the virtual MME, the operator's network can be adjusted according to capacity needs. A flexible and manageable network means that software upgrade and expansions can be rolled out quickly. This enables SoftBank to launch new services faster and more efficiently, with shorter lead times and lower capex and opex. In addition, this Cloud Platform can support SoftBank in the deployment of future applications, and meets the requirements of the Internet of Things and 5G.

2.2.3. Vodafone, Netherlands has deployed the country's first cloud-based and fully virtualized Voice over LTE (VoLTE) and Wi-Fi calling solution. Wi-Fi calling enables operator to provide voice services in more locations, such as indoor environments like basements, by complementing macro network coverage. VoLTE offers fast call set-up times and high-definition (HD) voice quality while facilitating a broader range of IP-based communication capabilities, such as video calling over LTE and multi-device support. The solution is based on a commercial Network Functions Virtualization (NFV) deployment of IP Multimedia Subsystem (IMS) and Evolved Packet Core (EPC). The complete cloud-based solution also includes Virtual Network Functions (VNF) for Wi-Fi calling, policy control and application server domain.

2.2.4. Caribbean operator Digicel has deployed a complete network functions virtualization (NFV) solution to the 3G core network. The new 3G network will enable Digicel to offer increased speed as well as improved network quality and customer experience. Virtual Evolved Packet Core is fully integrated with the operator's native network. It supports 2G, 3G and is ready for LTE.

2.2.5. Australian telecom operator Telstra plans to deploy a full stack telecom cloud solution consisting of virtual EPC and virtual IMS. The deployment of the solution will provide Telstra's network with a 5G-ready core and will help the network scale as Internet of Things (IoT) adoption increases. As 4G and 5G Radio Access Network (RAN) speeds increase to many gigabits per second and latency decreases, the core network needs to evolve from today's relatively static, centralized architecture to an architecture that can elastically centralize some functions and distributes others to deliver flexibility, efficiency and low latency.

3.0 Unique Security Implication of Cloud

Although clouds allow service providers to avoid start-up costs, reduce operating costs, and increase their agility by immediately acquiring services and infrastructural resources when needed, their unique architectural features also raise various security and privacy concerns, which are in addition to those inherited from the legacy systems. The challenges and concerns, which are unique to cloud environment and need to be addressed to make cloud computing a true value proposition are discussed below.

3.1. Extensibility and Shared Responsibility

Cloud providers and clients (TSPs) must share the responsibility for security in cloud computing environments, but sharing levels will differ for different service models, which in turn affect cloud extensibility. A typical responsibility sharing in various cloud service models has been depicted in Figure. 2.

- In SaaS (Software as a Service), cloud providers typically enable services with a large number of integrated

features, resulting in less extensibility for customers. Cloud providers are more responsible for the security of application services, more so in public than private clouds where the client telecom organization might have stringent security requirements and provide the needed enforcement services. Private clouds could also demand more extensibility to accommodate customized requirements.

- In PaaS (Platform as a service), the goal is to enable developers to build their own applications on top of the platforms provided. Thus, customers are primarily responsible for protecting the applications they build and run on the platforms. Providers are then responsible for isolating the customers' applications and workspaces from one another.
- IaaS (Infrastructure as a service) is the most extensible delivery model and provides few, if any, application-like features. It's expected that the consumers secure the operating systems, applications, and content. The cloud provider still must provide some basic, low-level data protection capabilities.

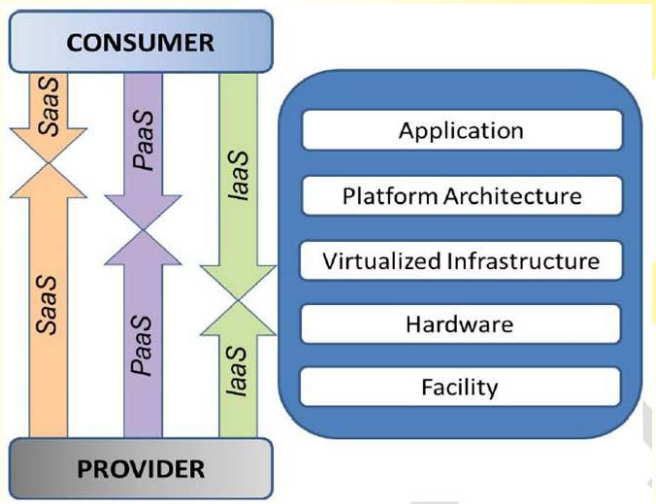

Fig. 2: Security responsibility in different cloud service models [source: NIST SP500-299]

3.2. Outsourcing Data and Applications

When the operation critical data, subscriber and other commercial data, is moved to the Cloud by the TSPs, that data is required to be accessed frequently to provide the services with high availability and QoS. The challenge is to ensure that only authorized entities gain access to the data available in the cloud. In the cloud environment, reliance has to be placed on third parties to make decisions about data and platforms in ways never seen before in computing. It is critical to have appropriate mechanisms to prevent cloud providers from using customer's data in a way that hasn't been agreed upon. It seems unlikely that any technical means could completely prevent cloud providers from abusing customer data in all cases, so we need a combination of technical and non-technical means to achieve this. Clients need to have significant trust in their provider's technical competence and economic stability. The cloud provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees who can exploit weaknesses in the data security model to gain unauthorized access to data. This involves the use of strong encryption techniques for data security both in storage & exchange and fine-grained authorization to control access to data.

First wave of cloud computing was created by Amazon Web Services (AWS), which was launched with a few simple compute and storage services in 2006. A decade later, AWS is operating at an $11 billion annual turnover.

3.3. Multi-Tenancy through Virtualization

Multi-tenancy is another feature unique to clouds, especially in public clouds. Essentially, it allows cloud providers to manage resource utilization more efficiently by partitioning a virtualized, shared infrastructure among various customers. As shown in Figure. 3 below, virtualization is an important enabling technology that helps abstract infrastructure and resources to be made available to multiple clients as isolated Virtual Machines (VMs). A hypervisor or VM monitor is a piece of platform-virtualization software that lets multiple operating systems run on a host computer concurrently.

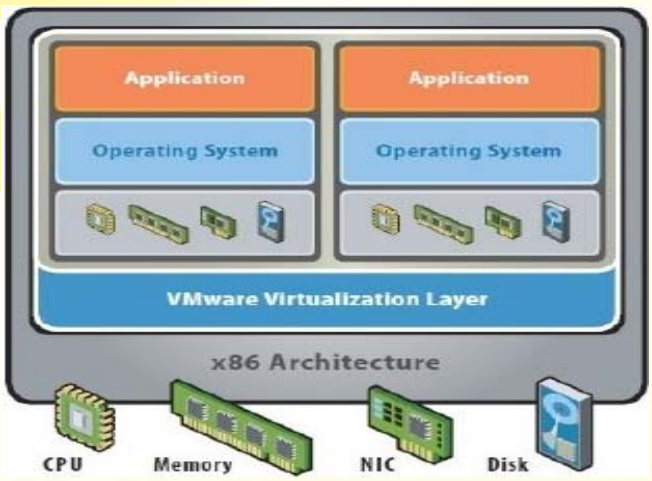

Fig. 3: Multi-tenancy in Cloud computing [source: cornerstone.IT]

Although this provides a means to generate virtualized resources for sharing, presence of such technology also increases the attack surface. We need mechanisms to ensure strong isolation, mediated sharing, and secure communications between VMs. This could be done using a

flexible access control mechanism that governs the control and sharing capabilities of VMs within a cloud host.

3.4. Heterogeneity

Heterogeneity in clouds comes in different forms. Cloud providers use various hardware and software resources to build cloud environments. To some extent, resource virtualization achieves high-level system homogeneity, but the same infrastructure being used to support different tenants with different protection and system requirements can generate difficulties. In a multi-tenant environment, the protection requirements for each tenant might differ, which can make a multi-tenant cloud a single point of compromise. In addition, each tenant could have different trust relations with the provider—and some tenants could actually be malicious attackers themselves— thus generating complex trust issues.

4.0 Security Threats in Telecom Networks on Clouds

With NFV, a number of security issues arise in telecom networks besides the generic security issues applicable to IT applications on cloud, e.g. data security, network security, identity management etc. These threats can be leveraged using some available mitigation techniques and also through other emerging solutions. This section presents critical security threats that exist in the NFV infrastructure in telecom networks.

4.1. Threats in multi-cloud deployments

Sometimes, it may happen that a telecom operator might subscribe to an IaaS from one cloud provider, couple it with a PaaS from another cloud provider, and acquire various pieces of SaaS from a third cloud provider. The assumptions that each of these cloud providers make in building the services can severely affect the emergent trust and security properties of the network of the TSP. In such a scenario a cloud service uses APIs (Application Programming Interfaces) to communicate with other cloud services. As a result, the security of APIs has a direct impact on the security of the overall service provided by the telecom operator. In a worst case this may cause TSPs to loose confidential information related to their customers.

4.2. Mobile Botnet Threat to vMME

In virtual MME scenario, an attacker could create a botnet army by infecting many mobile devices with a “remote-reboot” malware, enabling the attacker to instruct the malware to reboot all devices at the same time. The simultaneous rebooting of all devices causes excessive “malicious” attach requests and results in a signalling storm, putting vMME under DDoS attack. In response to the attack, the orchestrator may instantiate a new VNF to scale-out the vMME function to sustain the surge in the signalling traffic and to ensure service availability while the attack is being investigated.

4.3. Isolation Failure Threat

In this attack scenario, the attacker first compromises one VNF by gaining access to its operating system. Using tools and VNF network connectivity with the cloud management network, the attacker gains access to the hypervisor management API and then the attacker breaks into the hypervisor to cause great impact. These attacks are possible due to the improper isolation between hypervisors and VNFs.

4.4. Insecure VNF Migration

Sometimes, it may be required to move a VNF of a telecom operator from one location to another location. Live migration of VNFs exposes the contents of the VM state files to the network. An attacker can access data illegally during migration, transfer a VNF to an untrusted host or create and migrate several VNFs causing disruptions or DoS (Denial of service). These attacks mainly occur due to inappropriate access control policies, unprotected transmission channels and vulnerabilities in the migration module.

4.5. DNS Amplification Attack

A telecom NFV infrastructure (NFVI) hosts a virtual DNS server as a component of a virtual evolved packet core (vEPC). The NFVI orchestrator is able to deploy additional virtual DNS servers if the traffic load increases. In this attack scenario, an attacker may spoof IP addresses of a number of victims and launches a high number of malicious DNS queries using the spoofed IP addresses. In response to such an attack, the orchestrator will instantiate new VMs to scale-out the vDNS function to accommodate more queries. Accordingly, multiple recursive DNS servers will respond to the victims that will ultimately receive amplified DNS query responses, which may result in its service disruption or unavailability.

5.0 Counter measures

These threats can be leveraged using some available mitigation techniques discussed below and also through other emerging solutions.

5.1. Hypervisor Virtual Network Security

The hypervisor enables virtualization between underlying hardware and VMs. Telecom networks in the cloud use SDN to enable connectivity among VNFs and also with outside networks. Security of these elements is a must in order to protect the whole infrastructure. One of the security best practices is to keep the hypervisor up-to-date by regularly applying the released security patches. Failure to do that would result in exposure to security risks in the future. Another best practice is to disable all services that are not

in use. For example, Secure Shell (SSH) and remote access service may not be needed all the time; therefore, it would be a good idea to enable these services only when needed.

5.2. Security Zoning

To prevent a VNF from impacting other VNFs or hosts, it is a good practice to separate VM traffic and management traffic. This will prevent attacks by VMs tearing into the management infrastructure. It is also a good idea to separate the Virtual Local Area Network (VLAN) traffic into groups and disable all other VLANs that are not in use. Likewise, VNFs of similar functionalities can be grouped into specific zones and their traffic should be isolated. Each zone can be protected using access control policies and a dedicated firewall based on its needed security level.

5.3. Remote Attestation

The remote attestation technique can be used to remotely verify the trust status of a NFV platform. The concept is based on boot integrity measurement leveraging Trusted Platform Module (TPM), as mentioned earlier. Remote attestation can be provided as a service, and may be used by either the cloud provider or a consumer to verify if the platform has booted in a trusted manner. Practical implementations of the remote attestation service include the open cloud integrity tool (openCIT), an open source software hosted on GitHub.

6.0 Challenges and Ongoing works

Despite the countermeasures described above, there are still open security challenges that are yet to be addressed. One of the security challenges is to securely manage and monitor VNFs by maintaining their configuration and state information during migration. This can be difficult to perform due to the dynamicity and elasticity of VNF operations in cloud environments.

At the moment, attestation technologies only provide the boot time attestation. This does not guarantee prevention of run time modification or prevent tampering with the system's critical components, and such modification would only be detected when the system is rebooted. Run time attestation is still an open research area that needs to be explored further. There is also a strong need to develop a comprehensive security architecture to take care of these security challenges in NFVI. To achieve these goals, network operators and vendors need to work together to form a vibrant security eco-system. New standards, testbeds, and proofs of concept would serve as a catalyst for securing the NFV infrastructure. The services in this new virtualized environment are rapidly evolving, and in turn create new opportunities for innovation.

There are a number of ongoing research projects in the NFV security domain aiming to provide security and resiliency of the NFV infrastructure. The European H2020 Arcadia project1 has the objectives of detecting, exploring, and understanding security events in NFVI by service chain performance analytics to detect anomalistic behaviour of the network functions. The 5G Ensure project2 envisions securing future 5G networks that will rely on NFVI. It aims at developing security enablers consisting of privacy, trust, and virtualization isolation functions for 5G networks. OPNFV, an open source project from the Linux Foundation3, has a dedicated security group working on vulnerability management to develop network security functions for NFV.

7.0 Conclusion

Use of Cloud based resources is a recent paradigm that allows telecom operators to roll-out services in a cost effective manner. While there are numerous security risks, threats, and vulnerabilities associated with telecom networks on cloud, reliance is on cloud providers, telecom operators and end users to implement satisfactory countermeasures to keep cloud based telecom implementation an optimal option. As hackers and cybercriminals continue to get more sophisticated and educated in their methods of hacking, Telecom Equipment Manufacturers, TSPs and Security Experts must continue to find ways to protect the cloud infrastructure to address the growing concerns. As more methods are discovered, more solutions will be provided in creating security measures to strengthen telecom networks on cloud.

References:

1. ITU-T Recommendation X.1601 "Security Framework for Cloud Computing," Oct. 2015
2. NIST SP 800-145 "NIST Definition of Cloud Computing," Sept. 2011
3. NIST SP 500-299 "NIST Cloud Computing Security Reference Architecture," (Draft) May 2013
4. CSA Guide "Security Guidance for critical areas of focus in cloud computing V3.0", 2011
5. Dimitrios Zissis, Dimitrios Lekkas "Addressing cloud computing security issues" Elsevier Future Generation Computer Systems 28(2012) 583-592
6. Hamza Ahmed "Cloud computing security threats and countermeasures" International Journal of Scientific and Engg. Research Volume 5 Issue7 July 2014
7. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez "An analysis of security issues for cloud computing" Journal of Internet services and applications, 2013
8. Hardening of VMs-blog.govplace.com/2009/12/virtualization-security/
9. "Cloud RAN & Next generation mobile network", Heavy Reading, April 2017
10. Shankar Lal, Tarik Taleb, and Ashutosh Dutta "NFV Security threats & best practices" IEEE communications Magazine, 2017
11. https://www.ericsson.com/en/networks/topics/nfv
12. "Security Position Paper Network Function Virtualization" Cloud Security Alliance, 2016

Activities at NTIPRIT (JUL-17 to SEP-17)

1. Interaction meeting of ITS-2015 batch Officer Trainees with Hon'ble Minister of State (IC) for Communications at Sanchar Bhawan, New Delhi. Information is available at cover page.

Group photo with Hon'ble Minister

2. Hindi Karyashala (27-09-2017)

   One day Hindi Karyashala (workshop) was organized in NTIPRIT on 27-09-2017. Officers/officials of NTIPRIT participated in karyashala.

Glimpse of Hindi Karyashala

3. Induction Training of the following batches of Officer Trainees of ITS/BWS was conducted during the period:

   i. ITS-2015 batch (36 officers)

   ii. BWS-2015 batch (1 officer)

   iii. ITS-2014 batch (17 officers)

   Various training programs like technical modules and Field attachment of ITS/BWS were conducted during this period as per respective training calendar.

4. In-service training courses for DoT Officers were conducted at NTIPRIT on the following topics:

   i. 2 days, in-service training course on "Role of Telecom in Disaster Management", (29-30 August, 2017) [14 Participants]

हिंदी पखवाड़ा–2017

दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली में 14 से 28 सितंबर, 2017 तक हिंदी पखवाड़े का आयोजन सफलता एवं उत्साहपूर्वक किया गया। पखवाड़े का शुभारंभ श्री लव गुप्ता, वरिष्ठ उप महानिदेशक (टी.ई.सी.) द्वारा दीप प्रज्वलित कर किया गया। इस अवसर पर श्री गुप्ता जी ने माननीय गृह मंत्री का संदेश पढ़कर सुनाया। हिंदी पखवाड़े के दौरान कुल 10 प्रतियोगिताओं का आयोजन किया गया। पखवाड़े के दौरान आयोजित प्रतियोगिताओं में अधिकारियों/कर्मचारियों ने बढ़–चढ़कर भाग लिया।

समारोह का समापन श्री लव गुप्ता, वरिष्ठ उप महानिदेशक (टी.ई.सी.) की अध्यक्षता में सम्पन्न हुआ जिसमें सभी विजेताओं को पुरस्कार राशि एवं प्रशस्ति पत्र प्रदान किए गए। उन्होंने सभी उपस्थित अधिकारियों/कर्मचारियों को हिंदी के प्रचार–प्रसार हेतु अधिक से अधिक योगदान प्रदान करने के लिए प्रेरित किया। इस पखवाड़े के दौरान दिनांक 26.09.2017 को एक हिंदी कार्यशाला का आयोजन किया गया। कार्यशाला के अतिथि वक्ता श्री नगेन्द्र सिंह, तकनीकी निदेशक (राजभाषा विभाग) द्वारा कंप्यूटर पर यूनिकोड एनकोडिंग सक्रिय करने, गूगल–ट्रांसलेशन, गूगल वॉइस टाइपिंग, ई–महाशब्दकोश, श्रुतलेखन सॉफ्टवेयर–हिंदी में डिक्टेशन एवं कार्यालय कार्यों में हिंदी का ज्यादा से ज्यादा प्रयोग करने आदि के बारे में विस्तार से बताया गया।

हिंदी पखवाड़ा–2017 की झलकियाँ

Approvals from JUL-17 to SEP-17

Sl. No.	Name of the Manufacturer/Trader & Name of Product & Model No.
A	Tejas Networks Ltd
1	STM-4 synchronous multiplexer for TM, ADM and multi-ADM application, TJ1400(STM-4)
2	STM-1 synchronous multiplexer, TJ1400(STM-1)
B	Vishal Telecommunications Pvt. Ltd
3	IP Media Gateway, I-Gate 4000 Pro
C	NEC India Pvt Ltd
4	PABX for Network Connectivity, SL2100
D	Sunren Technical Solutions Pvt Ltd
5	Group 3 Fax Machine/Card, ProXpress M3370FD
6	Group 3 Fax Machine/Card, ProXpress M3870FD
7	PABX For Network Connectivity, ST006

Important Activities of TEC during JUL-17 to SEP-17

New GRs/IRs issued:

- GR on SAR measurement system for wireless communication devices used in close proximity to the human body (frequency range of 30 MHz to 6 GHz)

DCC meeting conducted for:

- GR on PABX
- GR on Raw material for manufacturing optical fibre cable
- GR on Multi service optical transport network(OTN) platform with DWDM bearer transport system for metro and core network application
- GR on Electronic Telephone Instrument
- GR on Asymmetrical Digital Subscriber Line 2+ system for central office & remote office applications
- IR on PABX for network connectivity, IR on SIGTRAN
- Test procedure for measurement of electromagnetic fields from base station antenna.

Sub DCC meeting conducted for:

- GR on Network function virtualization based CPE
- GR on Server
- IR on IVRS
- IR on MRTS subscriber unit, IR on MRTS base station
- SR on Audio conferencing

Representation of TEC in Training/Seminar/ Meetings

- Meeting of the quality of service development group ITU-T, SG-12 in South Africa
- Remote participation in ITU-T SG-17 meeting
- 4th meeting of Japan India JWG in Japan
- ITU-APT conference on 5G
- Workshop on ERMV w.r.t. PPDR at NDMA Delhi
- IXIA/INVAS Telco summit in Delhi
- 10th Annual summit on cyber and network security in New Delhi
- Workshop on 5G at Samsung R & D centre, Bengaluru

Brief About TEC

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support to DOT on technology issues
- Testing & Certification of Telecom products

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

For more information visit TEC website

www.tec.gov.in

Other Activities

- Meeting of NSG-5 & NWG-5 in TEC
- Technical presentations on security aspects of IoT, Cloud, 5G, SDN/NFV, Big data by M/s Huawei in TEC organised by DDG(SA), DoT HQ.
- Technical presentation on "5G" by M/s Ericsson in TEC
- Workshop on Global standardization updates and global best practices in testing & certification by M/s Ericsson in TEC
- Testing w.r.t. Technology Approval for CDOT Wi-Fi AP in CDoT, Bengaluru
- Two new division 'Telecom Certification' and 'Standardization' were formed in TEC.

टी ई सी संचारिका : दूरसंचार अभियांत्रिकी केन्द्र
नवम्बर 2017 : खुर्शीद लाल भवन
भाग 21 : जनपथ
अंक 4 : नई दिल्ली–110001

Editor : Ram Lal Bharti, DDG (NGS) Phone : 23321288 Fax : 23318724 E-mail : ddgs.tec@gov.in

Printed at : Yugantar Prakashan Pvt. Ltd., New Delhi; M: 9811349619