ISO 9001 : 2008

TEC

TELECOMMUNICATION ENGINEERING CENTRE

TEC

टी ई सी संचारिका

NEWSLETTER

Vol. 22 JULY 2018 ISSUE 3

दूरसंचार विभाग की हिंदी सलाहकार समिति की बैठक

In this Issue

दूरसंचार विभाग, संचार मंत्रालय की हिंदी सलाहकार समिति की बैठक दिनांक 29 मई, 2018 को रायपुर (छत्तीसगढ़) में माननीय संचार राज्य मंत्री (स्वतंत्र प्रभार) श्री मनोज सिन्हा जी की अध्यक्षता में हुई। इस बैठक में दूरसंचार विभाग और इसके नियंत्रणाधीन उपक्रमों/संगठनों/कार्यालयों के प्रमुख तथा अन्य उच्चाधिकारी आदि शामिल हुए। बैठक में दूरसंचार अभियांत्रिकी केंद्र का प्रतिनिधित्व श्री महाबीर प्रसाद सिंघल, वरिष्ठ उप महानिदेशक द्वारा किया गया। माननीय अध्यक्ष महोदय ने अपने संबोधन में विज्ञान और तकनीकी क्षेत्र में यथासंभव सरल, सुबोध एवं आम बोलचाल की भाषा हिंदी के प्रयोग की आवश्यकता पर बल दिया। बैठक में संयुक्त सचिव (प्रशासन) एवं सदस्य—सचिव ने दूरसंचार विभाग में राजभाषा नीति के कार्यान्वयन की दिशा में किए जा रहे विभिन्न प्रयासों के बारे में सभी सदस्यों को अवगत कराया। विशेष सचिव ने संबोधित करते हुए कहा कि हाल ही के वर्षों में हमारा देश विश्व के सबसे तेजी से विकास कर रहे दूरसंचार बाजार के रूप में उभरा है और हिंदी अपनी सरलता एवं लोकप्रियता के कारण विकास के पथ पर निरंतर अग्रसर है।

श्री मनोज सिन्हा जी, माननीय संचार राज्य मंत्री (स्वतंत्र प्रभार) हिंदी सलाहकार समिति के विभिन्न सदस्यों के साथ बैठक का शुभारंभ करते हुए

संसदीय राजभाषा समिति की दूसरी उप समिति द्वारा निरीक्षण

संसदीय राजभाषा समिति की दूसरी उप समिति द्वारा दिनांक 15 जून, 2018 को पहली बार दूरसंचार अभियांत्रिकी केंद्र के कार्यालय के कामकाज में 2017–18 के दौरान राजभाषा हिंदी के प्रगामी प्रयोग में हुई प्रगति का निरीक्षण नई दिल्ली में सफलतापूर्वक किया गया । उक्त बैठक में दूरसंचार अभियांत्रिकी केंद्र से श्री महाबीर प्रसाद सिंघल, वरिष्ठ उप महानिदेशक, श्री राम लाल भारती, उप महानिदेशक (एन.जी.एस.) और श्रीमती नीलम सिंघल, उप महानिदेशक (पी&टी) तथा दूरसंचार विभाग की तरफ से श्री संजीव गुप्ता, उप महानिदेशक (परियोजना प्रबंधन) और श्री पी. सी. विश्वकर्मा, संयुक्त निदेशक (राजभाषा) ने प्रतिनिधित्व किया। निरीक्षण बैठक माननीय डॉ. सत्यनारायण जटिया जी, उपाध्यक्ष, संसदीय राजभाषा समिति की अध्यक्षता में आयोजित की गई ।

समिति के उपाध्यक्ष डॉ. सत्यनारायण जटिया जी का स्वागत करते हुए श्री महाबीर प्रसाद सिंघल, वरिष्ठ उप महानिदेशक, टीईसी

संसदीय राजभाषा समिति की दूसरी उपसमिति द्वारा निरीक्षण
15 जून 2018, नई दि
भारतीय
डॉ. प्रसन्न कुमार पाटसाणी
डॉ. सत्यनारायण जटिया
लक्ष्मी नारायण यादव

समिति के उपाध्यक्ष डॉ. सत्यनारायण जटिया जी, सांसद राज्यसभा और संयोजक डॉ. प्रसन्न कुमार पाटसाणी जी, सांसद लोकसभा के साथ दूरसंचार अभियांत्रिकी केंद्र एवं दूरसंचार विभाग के अधिकारी गण

डॉ. प्रसन्न कुमार पाटसाणी जी दूरसंचार अभियांत्रिकी केंद्र द्वारा लगाई गई प्रदर्शनी का अवलोकन करते हुए

Application Security

1.0 Introduction

Thousands of new applications hit the market each week. Application either through Mobile handset, web, PCs, tablets provides an array of service which may contain user personal information and/or sensitive commercial information. With new applications, new security vulnerabilities are also discovered every day in commonly used applications. This vulnerability can put personal data of user at risk. An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. Once an attacker has found a flaw, or application vulnerability, and determined how to access it, it can exploit the application vulnerability to facilitate a cyber-crime. These crimes target the confidentiality, integrity, or availability (known as the "CIA") of resources possessed by an application, its creators, and its users.

Application security, or "AppSec," is what an organization does to protect its critical data from external threats by ensuring the security of all of the software used to run the business, whether built internally, bought or downloaded. Application security helps identify, fix and prevent security vulnerabilities in any kind of software application. Security measures in mobile apps involves security at various levels i.e. Application, network and host levels which is being described in this article.

2.0 Need for Mobile Application Security

Security of applications is critical due to the following reasons:

2.1 Storage and Processing of Sensitive Data: Mobile devices are being used to access a range of services, from social networking, banking, ticketing, and shopping to corporate applications such as email, enterprise resource planning (ERP), customer relationship management (CRM), and calendar and address book applications. The applications store and transmit a lot of sensitive personal and corporate information, such as login credentials, credit card details, private contact entries, invoices, and purchase orders. If developed insecurely, these applications could potentially disclose sensitive information.

2.2 Non transparent Use of Mobile Devices: Using personal phones for corporate purposes makes it difficult to enforce corporate policies and restrictions on these devices. Also, an attacker can more easily compromise personal devices than corporate- issued devices, which are locked down using far more draconian measures. Sensitive corporate applications and data on unmanaged personal devices open up security risks, such as exposure of confidential corporate information through lost or stolen phones, data interception and manipulation through Wi-Fi sniffing, and man-in-the-middle attacks at public Wi-Fi hotspots.

2.3 Regulatory requirements: Around the world, countries have their own regulatory requirements for enterprises that manage sensitive and confidential customer data such as personally identifiable information, personal health information, cardholder information, and financial information. Hence organizations dealing with such information must mandate use of minimum security requirements.

3.0 Mobile Application Security

Currently Smartphone have become incredibly important among people around the world are more than communication devices. They are like a personal computer, with more memory and processing power than your laptop of just a few years ago. Hence they have become the most targetable sources for hackers and malicious program.

As per GSMA statistics, total number of mobile subscription worldwide is 5108 million approx. till November 2017. A recent study from Veracode found the average global enterprise has approximately 2,400 unsafe applications installed on employees' mobile devices. Security researchers from antivirus software firm G Data have discovered that more than 750,000 new malicious apps have sprung out during the first quarter of this year, with estimates the total number will grow up to a staggering 3.5 million by the end of 2017.

3.1 Security Issues in Mobile Applications

3.1.1. Threat Vectors: Many threat vectors for infecting personal computers arise from social-engineering attacks that bypass anti-virus defenses. Similar techniques are used in the smartphone and tablet world by deceiving users into installing malicious apps. Examples include apps that gather personal information, track location, and charge accounts by sending text messages to premium-rate numbers. Using a mobile device to access corporate email or other resources also extends the threat to the organization, including the theft of sensitive data. While viruses and malware targeting mobile devices would share many of the same goals as on the PC, the enhanced capabilities of these devices present expanded attack surfaces through sensors such as GPS, accelerometer, camera, microphone, and gyroscope. Recently, Kaspersky Lab discovered a new threat involving the photo-scanning of Quick Response(QR) codes. QR codes are 2-D matrix barcodes increasingly used in advertising and merchandising to direct mobile-phone users to a website for further information on the tagged item.

3.1.2. Security Issues in Mobile Applications Platforms: Since more sensitive data now resides in mobile platforms, hackers are gradually shifting their attention towards mobile environment and its platforms. Currently various types of platforms exist to deploy mobile applications with different private policies. Development of Mobile application on various platforms is based on functional and non-functional requirements. Also the security within each platform such as Motion BlackBerry OS, Apple iOS, Google Android, Microsoft Windows Phone is different from one another. Hence mobile platforms play an important role for maintaining, effecting the aspect of application security.

a. Security Issues in Android: As per reports, it has been stated that 2016 was the year with the most malware appearances on Android devices. Experts estimate that 9468 new malware appear daily on average. This means that a new malware appears every 9 seconds.

Android is developed as an open source model. Android developers are free to add to the API, use third-party APIs, and distribute apps through any means as per their convenience. While all Android apps must be signed with a certificate, developers can create their own certificates without using a signature from duly certified certificate authority. Android provides the capability for greater application security than iOS, but based on security model of "trust them". Due to which a number of back doored/ malicious applications have been published to the Android app market and have been distributed to users.

Android grants permissions to resources on a per-application basis during the installation of the application. The user is given a one-time option to install/not install the application after reviewing the resources requested by the application, thereby granting all the permissions or not installing the application at all. Some apps require dangerous combination of permissions which can create threat to user privacy data.

In android, preferences are stored unencrypted: application and system preferences, including in some cases authentication information, credentials, and tokens, are also stored completely unencrypted on the device's file system. While this is not normally available without the user being prompted, an attacker with access to the device file system would be able to read this sensitive information.

All android applications have their own unique identity, and there was a vulnerability that allowed identities to be copied so that one application could impersonate another. This Fake ID breach allowed malicious applications to be recognized as a trusted one by the user without the user knowing about it. This could potentially allow malicious software to steal user information from a trusted application and even take control of the security mechanisms on a device. This problem arises from the Android package installer not verifying the validity of a chain of certificates.

Including these, various real world vulnerabilities have been identified in Android OS and developers are trying to fix those vulnerabilities in security updates.

b. Security Issues in IOS: Apple's "trust us" model controls security from malicious apps by providing only one outlet for app distribution and by tightly controlling the iOS Software Development Kit (SDK). Developers submitting apps for distribution must register with Apple to obtain certificates to build and deploy apps. All apps must be signed with the certificate assigned by Apple. Apps must be built using Xcode, Apple's own development tool, and apps may use only the official iOS SDK—no third-party software APIs. Apple's development program requires a yearly fee which must be kept up-to-date. Apple reserves the right to revoke the developer's certificate at any time, which will take any apps developed off the App Store and prevent the developer from distributing any further apps until restoration the certificate.

An additional security measure is sandboxing applications and their data stores. Sandboxing provides an app with its own process space and prevents the app from accessing other process spaces. Apple sandboxing does not prevent malicious attacks against an app, but it does limit the damage done by the hacked app to other parts of the device. iOS apps are not allowed to start or execute other apps.

It is said that IOS Security model is based on concept of "Trust Us" as it possesses complete control of app development for their platform, from the APIs and tools available for app development, to the distribution process, to the device itself. But in IOS all default security is at risk if the device is jail broken and it enables download of any unauthorized application which can create risk for system. Password protection mechanisms as adopted by IOS is mainly user interface based rather than enforced by kernel. Including this, certain vulnerabilities are also discovered in IOS and listed in CVE catalogue which allows remote attacker to execute arbitrary code or denial of service.

3.1.3. Insecure Data Storage: This risk occurs when sensitive data is stored on a device or when cloud-synced data is left unprotected. It's generally the result of not encrypting sensitive data, caching information not intended for long-term storage, allowing global file permissions, or failing to leverage best practices for a particular platform. This in turn leads to the exposure of sensitive information, privacy violations, and noncompliance.

3.1.4. Weak Server side controls: Failure to implement proper security controls such as patches and updates or secure configurations, changing default accounts, or disabling unnecessary backend services can compromise data confidentiality and integrity.

3.1.5. Insufficient Transport Layer Protection: Mobile applications use HTTP protocol for client-server communication which communicates all information in plain text. Even when they provide transport-layer security through use of the HTTPS protocol, if they ignore certificate validation errors or revert to plain-text communication after a failure, they can jeopardize security by revealing data or facilitating data tampering through man-in-the middle attacks.

3.1.6. Client Side injection: Apart from the known injection attacks such as XSS, HTML injection, and SQL injection applicable to mobile Web and hybrid apps, mobile apps are witnessing newer attacks such as abusing the phone dialler, SMS, and in-app payments.

3.1.7. Poor Authorization & Authentication: Authentication and authorization are critical controls for every mobile payment application since they not only authenticate the user but also authorize the payment. Weaknesses in authorization might allow impersonation attacks with stolen data such as stolen tokens being used by a different device and user other than that they were intended for. Attackers attempt to bypass authentication by spoofing biometric data, attempting to reset user credentials when they are lacking strong verification of the user with additional validation before reissuance of PINs and passwords.

3.1.8. Improper Session Handling: Improper session handling can be caused by failing to validate the session at logout, poor implementations of session expiration, issues with session tokens/cookies such as replay and hijacking of the sessions because of lack of protection of session data such as cookies in transit between client and servers.

3.1.9. Side Channel Data Leakage: Attackers could access sensitive data using side channels such as by installing malware on the device in order to control it remotely or to steal data from the device.

3.1.10. Broken Cryptography: This risk emanates from insecure development practices, such as using custom instead of standard cryptographic algorithms, assuming that encoding and obfuscation are equivalent to encryption, or hardcoding cryptographic keys into the application code itself. Such practices can result in a loss of data confidentiality or privilege escalation.

3.1.11. Escalated Privileges: Additional or excessive permissions acquired by application can sometimes effect privacy of individual and can cause application to get access to personal information. Also lack of proper implementation of sandboxing can cause any application to get access to unauthorised data.

3.1.12. Unlicensed and unmanaged apps: These apps can act as a blind spot for admins and thus placing the system and privacy of users at risk.

3.2 Countermeasures/Guidelines for Mobile Application Security:

Security in an application should be considered during development phase of application itself. Application development process can be prepared specifying the phases needs to be adopted while building secure application. It also reduces the cost of security implementation and fixing issues later. The countermeasures/guidelines which should be adopted for building a secure application are mentioned below:

3.2.1 Secure Application Development Cycle:

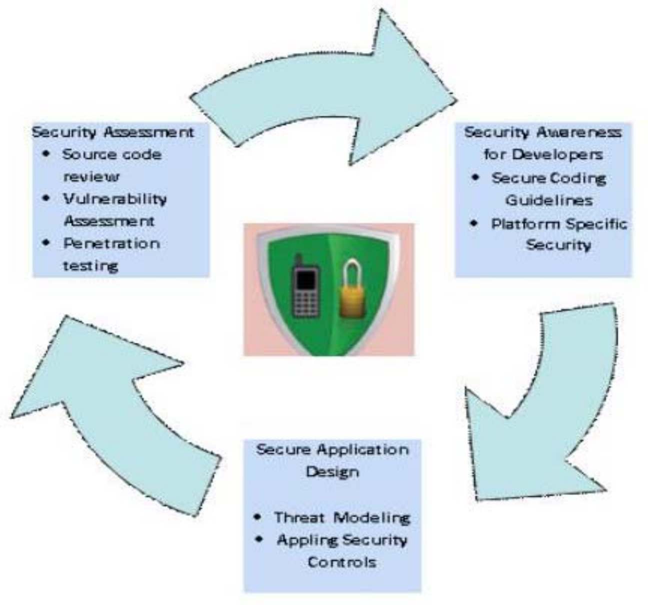
Security Assessment
• Source code review
• Vulnerability Assessment
• Penetration testing
Security Awareness for Developers
• Secure Coding Guidelines
• Platform Specific Security
Secure Application Design
• Threat Modeling
• Appling Security Controls

Fig. 1. Secure Application development process

i. Secure Application design:

As per business requirements: (1) users, (2) data sensitivity and (3) device types, Design considerations pertaining to (a) access control and privileges, (b) data encryption (in transit and local storage), (c) strong password and (d) account-lockout policies should be included in any mobile application design. An adequate threat-risk modelling of the application should also be considered in this phase to identify any security risks and determine the adequate security controls such as multifactor authentication, digital signature and TLS/SSL encryption based on criticality of application.

ii. Secure coding guidelines:

Developer of applications should be aware of following guidelines while developing an app:

a. Perform secure logging and error handling.

b. Follow the principles of least privilege with proper sandboxing implementation and isolation.

c. Validate input data both on client as well as server side and proper security controls must be implemented for input validations.

d. Avoid storing sensitive data on client devices unless absolutely necessary and use standard encryption algorithms with strong key values instead of default ones to encrypt sensitive data residing on devices or at the server backend.

iii. Security Assessment of applications:

Security assessment of mobile applications must be conducted before being released to production to attack surface or threats discovered during threat modelling have been addressed. This also addresses the issue arising from integration of different modules in application. This is done through security testing of applications. Security Testing is focused on the inspection of the application in the runtime environment in order to find security problems. Generally, for this purpose source code review tool (Static and dynamic analysis) along with vulnerability assessment and penetration testing tools can also be used.

3.2.2 Mobile device Security capabilities:

a. Trusted Execution Environment:

A TEE is a secure area that resides in the application processor of an electronic device, that runs a secure operating system in the main processor of a mobile device. The TEE includes key-storage and management functionalities. It also includes secure storage, which can be used to store transaction logs and authentication credentials in a private area. Separated by hardware from the main operating system, a TEE ensures the secure storage and processing of sensitive data and trusted applications. It

- implements an isolated computing resource in the mobile device,
- takes control over mobile vulnerable resources, particularly peripherals
- provides security properties to the executing critical application so that the application is immune to malicious software threats, and
- complements the security execution environment offered by an SE, including the provision of any encryption functionality

It protects the integrity and confidentiality of key resources, such as the user interface and service provider assets. A TEE manages and executes trusted applications built in by device makers, as well as trusted applications installed as people demand them. Trusted applications running in a TEE have access to the full power of a device's main processor and memory, while hardware isolation protects these applications from user-installed apps running in a main operating system. The software and cryptographic isolation inside the TEE protect the trusted applications contained within from each other.

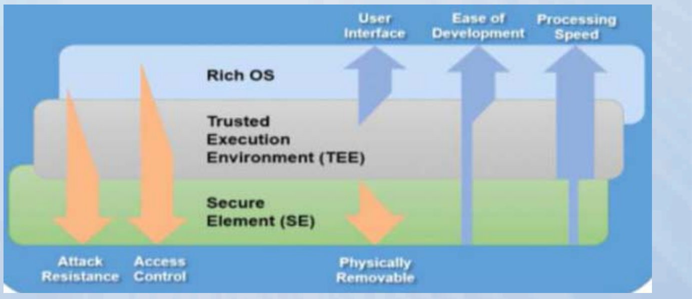

Fig. 2. Rich OS, TEE OS and SE positioning

A typical mobile with TEE has Rich OS & TEE OS, only TEE OS can access the application process which needs to be secured. Rich OS will access TEE OS through API which in turn will carry out the secure processing within TEE (in protected service area). Figure 2 depicts such a mechanism.

b. Secure Element / TPM (Trusted Platform Module)

A Secure Element (SE) is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. The TPM is an implementation of the functions defined in the TCG TPM 2.0 Library Specification. The TPM includes some RoT, shielded locations, and protected capabilities. In general, the TPM provides a set of functions and data that enable platforms to be trustworthy.

3.2.3 Guidelines for Mobile Application Security:

Risk factor in mobile device mainly has four stages such as application coding, Application distribution, Application Configuration and Configuration of device. Following steps should be adopted to maintain security in application:

i. Mobile have trusted execution environment inbuilt in their architecture. This can also be used to store critical applications such as financial applications etc.

ii. Secure element also along with TEE can be used to provide separate and secure space for critical and important applications.

iii. Mobile applications should be designed with built-in capabilities of Root/Jailbreak detection, tamper resistance against reverse engineering, multilayer authentication leveraging voice, fingerprinting, image, and geolocation.

iv. Application stores for different mobile device vendors use different security vetting processes. It's important to make sure applications aren't corrupted during the distribution process.

v. Temper detection and code obfuscation mechanisms should be implemented strictly in mobile handsets.

vi. Store the sensitive data properly

vii. Proper authentication mechanisms should be in place.

viii. Leveraging code obfuscation and anti-tampering to prevent reverse engineering.

ix. Use security testing tools such as Vulnerability assessment and penetration testing etc. in regular manner

x. Security and authenticity of 3rd party libraries should be validated. Binary testing tool can also help in security testing of 3rd party codes/libraries.

xi. A white-list of suitable, applicable and safe applications and software should be published within the organization and centrally imposed on all devices.

xii. Mobile devices should be controlled centrally to enable entity-wide configurations, remote data management, remote data recovery and data wipe.

4.0 Conclusions

Mobile application security not only includes just code running on devices but also other multiple factors such as device platform, cloud services, web services etc. A proper software development lifecycle should be adopted before app development and subsequently after its deployment. TEC is also going to establish security test lab which is having vulnerability assessment and penetration testing tool, Source Code review tool and binary testing tool which are capable of performing application tests during its various development and deployment phases. By adapting proper development lifecycle and subsequent proper security testing of any app, application vulnerabilities can be identified and can be eliminated well in advance before deploying and thereby resulting in considerable saving in investment.

Mandatory Testing and Certification of Telecom Equipments (MTCTE)

The Mandatory Testing and Certification of Telecom Equipments scheme will come into effect from 1st October 2018 and various actions under MTCTE scheme are underway including framing of ERs, development of MTCTE portal and designation of CABs.

TEC has finalised the Essential Requirements of most of the telecom products like Mobile devices, BTS, PABX, Soft switch, Transmission and Radio Equipments, Terminal Equipments etc. ERs for few more products are being finalised. The development of MTCTE online portal is in progress and trial version of portal is under test.

The CAB designation process is on and so far 16 CABs have been designated by the end of june-2018. To have the wider participation of Govt. bodies/Govt. organisations in the CAB designation, few relaxations in the eligibility conditions (i.e. Audited Financial Statements Application fees and NABL accreditation) have been provisioned on dated 18-06-2018.

TEC expects to have sufficient capacity within six months of starting certification process, and during this period, relaxation to submit test reports from any international accredited lab under ILAC network shall be available.

More details are available at

http://www.tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments-mtcte/

Activities at NTIPRIT (APR-18 to JUN-18)

1. **Interaction meeting of ITS-2016 and P&T BWS-2016 batch, Officer Trainees with Hon'ble Minister of State for Communications (MOS C (I/C)), Govt. of India at Sanchar Bhawan, New Delhi**

As part of Induction Training, interaction session of Officer Trainees of ITS-2016 and P&T BWS-2016 batch was organized, with Hon'ble Minister of State for Communications (MOS C (I/C)) at Sanchar Bhawan, New Delhi on 8th May, 2018. Hon'ble Minister, Sh. Manoj Sinha ji, addressed the Officer Trainees. In his Address, Hon'ble Minister, exhorted the Officer Trainees to develop capabilities in telecommunications sector to bring India at par with developed countries in the area of latest technologies, especially in 5G. Hon'ble Minister also suggested to include the topics on Emerging Technologies in ICT domain in Induction Training curriculum of ITS probationers. Hon'ble Minister blessed the young Officer Trainees with encouraging words of wisdom - to have clear Vision, Creativity, Passion to do & deliver, Integrity & Maturity while discharging their duties. Sh. Deepak Sinha, Member (S); Sh. Prabhash Singh, Member (T); Sh. Sunil Kumar, DG (Telecom); Sh. Debatosh Manna, Advisor (NTIPRIT); Sh. Rajesh Sharma, DDG (Training) DOT; Sh. H. S. Jakhar, DDG (Training) NTIPRIT; Sh. Subhash Chand, Director (Training) NTIPRIT were present during the deliberations.

Group Photograph with Hon'ble Minister

2. **Course on Cyber Security for ITS-2016 Batch (04-06-2018 to 22-06-2018)**

Three weeks classroom training on Cyber Security was conducted at NTIPRIT. During the course, the experts from government and private organizations in the domain of Cyber Security were invited to deliver the lectures and share the experiences in the cyber security domain. The Law Enforcement Agencies aspects were also explored to the trainees during the course. Officers were also, deputed to C-DAC, Noida for two days training on latest trends in Cyber Security form 18-06-2018 to 19-06-2018.

3. **Classroom Induction Training of the following batches of Officer Trainees of ITS/BWS and JTO probationers were conducted during the period**

i. ITS-2015 batch (34 officers), ii. ITS-2016 batch (34 officers), iii. BWS-2015 batch (1 officer), iv. BWS-2016 batch (3 officers), v. JTO-2016 Batch (2 officers).

Various training programs like technical modules and DoT attachment, TEC attachment, BSNL / MTNL attachment and Field Attachment (Stage –II) for ITS / BWS batches and field attachment with LSAs for JTO batch , 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. Training course on "Deployment issues in NGN", (09-10 May, 2018) [10 Participants],

ii. Training course on "Vigilance & Disciplinary Proceedings",(04-07 June, 2018) [8 Participant]

Approvals from APR-18 to JUN-18

Sl. No.	Name of the Manufacturer/Trader & Name of Product & Model No.
A	**Tejas Networks Ltd.**
1	STM-16 TM/ADM, TJ1400
B	**ECI Telecom India Pvt Ltd**
2	Digital Multiplexer (SDH) STM-4, BG20B
3	Digital Multiplexer (SDH) STM-4, BG30
4	Digital multiplexer (SDH) STM-16, XDM900
5	Digital Multiplexer (SDH) STM-4, XDM100
6	Digital Multiplexer (SDH) STM-1, MSDM
7	Digital Multiplexer (SDH) STM-16, XDM100
8	Digital Multiplexer (SDH) STM-16, XDM300
9	Digital Multiplexer (SDH) STM-4, NPT1020
10	Digital Multiplexer (SDH) STM-16, XDM100
C	**Bose Corporation India Pvt Ltd**
11	Terminal for Connecting to PSTN, EX-1280C
D	**Avaya India Pvt Ltd.**
12	PABX For Network Connectivity, IPO 500 V2
13	PABX For Network Connectivity, Avaya Aura Communication Manager
E	**Aspect Contact Centre Software India Pvt Ltd**
14	Systems Employing Computer Telephony Integration, DCP-00

Important Activities of TEC during APR 18 to JUN 18

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

GRs/IRs issued:

- GR on Unified Threat Management
- GR on Ethernet to E1 converter
- GR on Optical Fibre Drop Cable for FTTH applications
- GR on Self-supporting metal free aerial optical fibre cable (for hilly & rural areas)
- GR on Self-supporting metal free aerial optical fibre cable (for urban areas)

MATCOF meetings conducted for:

- Mandatory Testing Consultative Forum meeting was conducted for formulation of Essential Requirements for different types of products & their variants in TEC

DCC meeting conducted for:

- GR on Session Border Controller
- IR on Session Border Controller, SIGTRAN

Sub DCC meeting conducted for:

- GR on NFV CPE, IDS, IPS
- SR on IDMS

Representation of TEC in Training/Seminar/Meetings:

- ITU-T SG-5, SG-12 and SG-13 meetings at Geneva
- Remote participation in ITU-T SG-20 meeting held in Cairo & presented contribution
- Workshop on Security organised by ETSI at Sophia Antipolis, France
- Seminar on 'Internet of Things (IoT)' and '5G Technology - Evolution, Standards and Regulatory perspective' at DoT HQ, New Delhi
- Workshop on Building a foundation for quality devices with 5G certification at New Delhi
- Workshop on VM ware conclave on 5G at New Delhi
- Seminar on National Broadband summit at New Delhi
- Workshop on 5G organised by CDoT at Bangalore
- 3rd edition of Indo-EU Conference on standards and emerging technologies at New Delhi.

Study/white paper issued:

- Smart Environment and Pollution Control Domain

Other Activities:

- Meeting of NWG - 5, 11, 13, 17 & 20 in TEC
- 06 new Labs have been designated as CAB of TEC (M/s Intertek India Private Limited, New Delhi, M/s AB MSAI Research Labs Private Limited, New Delhi, M/s Nemko India (Test Lab) Private Limited, Faridabad, M/s SPECTRO Analytical Labs Limited Greater Noida, M/s Delhi Test House, Delhi and M/s UL India Private Limited, Gurugram)
- Technical presentations on Artificial Intelligence (AI) was given by M/s Ericsson on 16th May 2018 in TEC on occasion of World Telecommunication and Information Society Day (WTISD) with theme "Enabling the positive use of artificial Intelligence for all".
- A delegation comprising officers of DoT, TEC & ITI visited M/s ST Microelectronics premise's to see the IoT prototypes related to Smart Light System etc.

DISCLAIMER : TEC Newsletter provides general technical information only and it does not reflect the views of DoT, TRAI or any other organisation. TEC/Editor shall not be responsible for any errors, omissions or incompleteness.

Suggestions/feedback are welcomed, if any for further improvement.

टी ई सी संचारिका : दूरसंचार अभियांत्रिकी केन्द्र
जुलाई 2018 : खुर्शीद लाल भवन
भाग 22 : जनपथ
अंक 3 : 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