ISO 9001 : 2008

TEC

TELECOMMUNICATION ENGINEERING CENTRE

टी ई सी संचारिका

NEWSLETTER

Vol. 22 APRIL 2018 ISSUE 2

Synergy among PSUs and other organizations of DoT

In this Issue

The **"Strategic Plan"** for synergy among PSUs and other organizations of DoT was released by the Hon'ble Minister of State for Communications (Independent Charge) Shri Manoj Sinha on 22nd February 2018 in the National Media Centre, New Delhi. The Strategic Plan is for creating synergy among the public sector units (BSNL/MTNL/BBNL/TCIL/ITI) and other organisations of the Department of Telecommunications (DoT) including TEC and C-DoT.

In the inaugural session followed by the release of 'Strategic Plan' number of MoUs were signed among different PSUs/ Organisations of DoT as part of the Synergy. On this occasion TEC has also entered into an MoU with TCIL for "TEC Certification Recognition by Foreign Certification Bodies". The MoU was exchanged by Sr. DDG TEC and CMD TCIL in the august presence of the Hon'ble Minister of State for Communications (Independent Charge). Consequent to this, there has been some interest shown by Kuwait Ministry of Communications/ Regulator w.r.t the Certification of the telecom equipment by TEC. TEC & TCIL are working further in this respect.

दूरसंचार विभाग
Department of Telecommunications
Release of 'Strategic Plan', Signing of MOUs
Conference on 'Current and Emerging Opportunities for PSUs'
Chief Guest
श्री मनोज सिन्हा
Shri Manoj Sinha
Hon'ble Minister of State for Communications (Independent Charge)
Minister of State for Railways, Government of India
22nd February, 2018

(Releasing of Strategic Plan for Synergy among PSUs and other organizations of DoT by Shri Manoj Sinha, Hon'ble Minister of State for Communications)

Synergy……..: Continue from cover page

In the afternoon session, followed by the Inaugural session, a panel discussion with senior officers from the DoT and the PSUs was held on "Current and Emerging Opportunities for PSUs and other organizations". Shri M. P. Singhal, Sr. DDG TEC has participated as one of the eminent panelists in this session. During discussions various aspects of the strategic plan, available & emerging opportunities and implementation issues were thoroughly discussed.

Under the "Strategic Plan" released by the Hon'ble Minister of State for Communications (Independent Charge) the following are the important activities in which TEC has an active role to play: -

- TEC and C-DoT have to prepare Short Term (2018-19), Medium Term (2019-20) and Long Term (2020-21 onwards) "Technology Roadmaps" for policy formulation and technology guidance of DoT.
- TEC to lead a core Group of DoT which will bring out a Reference Document on "Roadmap for Smart Infrastructure".
- Preparation of GR/IR/SR by TEC as per the procurement plans of BSNL/MTNL/BBNL (100% availability of specifications by TEC, 6 months in advance, as per the procurement plans of the user organizations).

Inauguration by Hon'ble Minister

Addressing the session by Hon'ble Minister

Exchange of MoU between Shri M. P. Singhal, Sr. DDG, TEC and Shri Shri A. Seshagiri Rao , CMD, TCIL

Senior Officers from the DoT and the PSUs during a panel discussion on "Current and Emerging Opportunities for PSUs and other organizations"

Shri M. P. Singhal, Sr. DDG, TEC and Shri Vipin Tyagi, ED, CDoT

IMS Security

1.0 Objective

IP Multimedia Subsystem (IMS) is an architectural framework for offering multimedia and voice over IP services. IMS is access independent as it supports multiple access types including GSM, WCDMA, CDMA2000, WLAN, WiMAX, LTE, Wireline broadband and future access technologies. The IP Multimedia Subsystem (IMS) dates from 3GPP release 5 over a decade ago, but is now becoming a reality with the rollout of IMS based LTE networks. The IP Multimedia Subsystem standardized by 3GPP and 3GPP2 is a technology that merges both the cellular and internet technologies. It is an IP based network which provides the users a wide range of multimedia services such as audio, video and data over a single IP network. Because of open and distributed architecture of IP based networks it is easier for intruders to attack on these networks and access information, resources and services.

In the present study paper an attempt has been made to identify the various security threats associated with the IMS network. Based on the identified threats and challenges, certain countermeasures have also been discussed to protect the IMS services and resources from these threats.

As per GSMA, as on 9th March 2018 Voice and Video over LTE has been launched by 127 operators in 63 countries. (India – Reliance Jio, Airtel)

2.0 IMS Architecture

3GPP / TISPAN portrays IMS architecture as three separate layers i.e. the transport layer, the IMS layer and the service/ application layer. However, for this paper a simplified network architecture has been presented in figure 1 depicting how IMS is connected to EPC (evolved packet core) of the LTE network.

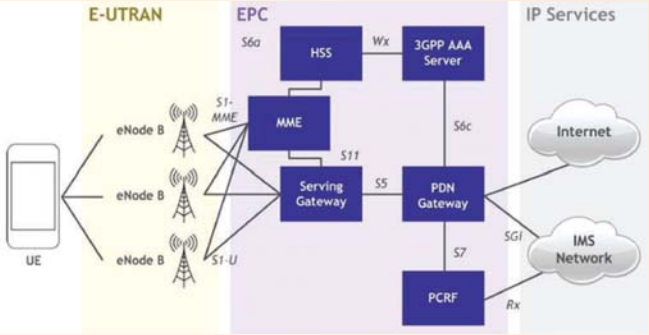


Figure 1—IMS with LTE Evolved Packet Core

2.1 Device Layer / User Equipment (UE)

User Equipment (UE) is the mobile terminal which may be a smartphone or tablet or any communication device which is authorized to be used in the network. An IMS powered UE has two main components Universal Integrated Circuit Card (UICC) and Session Initiation Protocol User Agent (SIP UA).

2.1.1. Universal Integrated Circuit Card (UICC)

Each UE must contain one UICC and each UICC may have one or more of the following modules.

i. Subscriber Identity Module (SIM): SIM identity information used by a GSM network.

ii. UMTS Subscriber Identity Module (USIM): USIM information used by a UMTS or LTE network.

iii. CDMA Subscriber Identity Module (CSIM) or Re-Useable Identification Module (R-UIM): identity information used by a CDMA network.

iv. IP Multimedia Services Identity Module (ISIM): ISIM identity information used by the IMS subsystem. ISIM contains the following:

a. IP Multimedia Private Identity (IMPI): IMPI is a global identity allocated by home network. IMPI contains home operator’s domain information.

b. IP Multimedia Public Identity (IMPU): IMPU acts like a telephone number which can either be a SIP URI (sip:<username>@<host>:<port>) or a tel URI as defined in RFC 39664 (tel:<country_code><national_destination_code><subscriber_number>).

c. Secret Key: This long secret key is used for user authentication and SIP registration.

Although MME performs very important functions like Authentication, Authorization, Bearer management functions including dedicated bearer establishment etc. no user plane traffic passes through it

2.1.2. SIP User Agent (SIP-UA)

SIP User Agent resides in the UE to transmit and receive SIP messages. SIP-UA provides basic telephony functionality. It plays two different roles:

i. User Agent Client (UAC): As a client to send SIP request

ii. User Agent Server (UAS): As a server to receive requests and send response

2.2 Transport Layer / Evolved Packet Core (EPC)

For VoLTE and IMS perspective two nodes are important in the Evolved Packet Core.

2.2.1. Public Data Network Gateway (PDN-GW)

PDN Gateway is responsible for allocating IP addresses to UEs. PDN-GW is also the point of communication between EUTRAN and non-3GPP services like internet. When IMS is used there can be more than one PDN-GW in the EPC one for internet and one for IMS.

2.2.2. Policy and Charging Rule Function (PCRF)

The PCRF provides real-time determination of what types of traffic are allowed under what conditions, and also determines how to account for this traffic (for billing purposes). Based on requests for IMS services, the PCRF also initiates the appropriate bearers. When a user initiate a VoLTE call PCRF checks if that user is allowed to start a VoLTE call or not and if it is allowed PCRF sets up dedicated bearer.

Interworking of 4G LTE IMS network with a "trusted" WLAN involves interfacing with a Trusted Wi-Fi Access Gateway (TWAG) function. TWAG terminates a layer 2 (e.g. Ethernet) interface from the WLAN and provides an S2a (GTP or Proxy Mobile IP based) interface to the P-GW or GGSN.

2.3 Control Layer / IMS Core

IMS core is responsible for session management and media control.

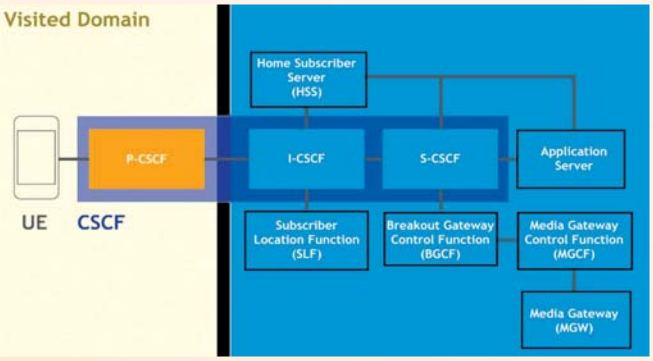

Visited Domain
Home Subscriber Server (HSS)
P-CSCF
I-CSCF
S-CSCF
Application Server
UE
CSCF
Subscriber Location Function (SLF)
Breakout Gateway Control Function (BGCF)
Media Gateway Control Function (MGCF)
Media Gateway (MGW)

Figure 2—IMS Core

IMS core has the following important nodes.

2.3.1. Call Session Control Function (CSCF)

CSCF is basically a collection of SIP servers responsible for establishing, monitoring, supporting and releasing multimedia sessions. It has three different functional elements which may or may not be separate physical entities.

i. **Proxy CSCF:** P-CSCF also known as SIP proxy is the initial point of contact from any SIP User Agent. It is assigned to an IMS terminal before registration, and does not change for the duration of the registration. It provides subscriber authentication and may establish an IPsec or TLS security association with the IMS terminal. This prevents spoofing attacks and replay attacks and protects the privacy of the subscriber.

ii. **Serving CSCF:** S-CSCF is a SIP server responsible for session control. It is always located in the home network. It uses Diameter protocol to interact with the HSS to download user profiles and upload user-to-S-CSCF associations. It handles SIP registrations, which allows it to bind the user location (e.g., the IP address of the terminal) and the SIP address. It is responsible for routing all signalling messages of the locally registered users. It enforces the policy of the network operator.

iii. **Interrogating CSCF:** I-CSCF is another SIP server located at the edge of an administrative domain. Its IP address is published in the Domain Name System (DNS) of other domains, so that remote servers can find it, and use it as a forwarding point for SIP packets to this domain. It queries the HSS to retrieve the address of the S-CSCF and assign it to a user performing SIP registration. It also forwards SIP request or response to the S-CSCF.

2.3.2. Home Subscriber Server (HSS)

HSS is a database that maintains user profile and location information and is responsible for name/address resolution. HSS is also responsible for authentication and authorization.

2.3.3. Subscriber Location Function (SLF)

SLF is responsible for assigning HSS to user in home network. To achieve this function SLF keeps track of all HSSes.

2.3.4. Breakout Gateway Control Function (BGCF)

A Breakout Gateway Control Function (BGCF) is a SIP proxy which processes requests for routing from an S-CSCF when the S-CSCF has determined that the session cannot be routed using DNS. It includes routing functionality based on telephone numbers.

2.3.5. PSTN / CS Gateways

PSTN/CS gateway interfaces with PSTN circuit switched (CS) networks. For signalling, CS networks use ISDN User Part (ISUP) (or BICC) over Message Transfer Part (MTP), while IMS uses SIP over IP. For media, CS networks use Pulse-code modulation (PCM), while IMS uses Real-time Transport Protocol (RTP).

i. **Signalling gateway (SGW)** interfaces with the signalling plane of the CS. It transforms lower layer protocols as Stream Control Transmission Protocol (SCTP, an IP protocol) into Message Transfer Part (MTP, an Signalling System 7 (SS7) protocol), to pass ISDN User Part (ISUP) from the MGCF to the CS network.

ii. **Media gateway controller function (MGCF)** is a SIP endpoint that does call control protocol conversion between SIP and ISUP/BICC and interfaces with the SGW over SCTP. It also controls the resources in a Media Gateway (MGW) across an H.248 interface.

iii. **Media gateway (MGW)** interfaces with the media plane of the CS network, by converting between RTP and PCM. It can also transcode when the codecs don't match (e.g., IMS might use AMR, PSTN might use G.711).

> **"Untrusted" WLAN access is performed via an entity called the evolved Packet Data Gateway (ePDG). ePDG is similar to a VPN concentrator that terminates the IPsec tunnels set up by the user device. The user handset uses DNS to look up the IP address of the ePDG and initiates the set up of the IPsec tunnel using IKEv2. The ePDG interfaces to the P-GW via the S2b interface.**

2.4 Control Layer / IMS Core

Applications and content services are hosted on application servers and Web servers. It also includes generic service enablers that manage service elements such as user groups and presence. These service elements connect to subscribers through the IMS core. The application layer supports most of the multimedia applications or application enablers, such as presence and location of the subscriber.

3.0 Security threats in IMS

IMS already has its security framework which is divided into two parts: access security and network security. Access security includes authentication related mechanisms and traffic protection between the user equipment (UE) and core network, which is specified in 3GPP TS 33.203. Network protection includes traffic protection between the network elements and also roaming and non-roaming scenarios, which is specified in 3GPP TS 33.210. But IMS is still vulnerable to several types of attacks like DoS and DDoS attacks. These attacks are a large number of random messages sent from single or multiple malicious nodes to overload network resources. Some of the security threats to IMS network are discussed below.

3.1. Access Layer threats

Access layer is the connection point between network-based services and client devices. It plays an important role in protecting other users, the application resources, and the network itself from human error and malicious attacks. Smartphones, tablets and laptops are key network entry points for security threats, which once connected allow a hacker to propagate infection to other endpoints on the IMS network. All these devices are the targets of threats such as viruses, worms, Trojan horses, Adware, Spyware and spam.

3.2. Transport Layer threats

One of the most common threats to the Transport Layer is from a flood of data packets that consume a network's entire bandwidth and cause it to perform poorly. This type of flood can occur using any of the available network protocols such as a TCP Flood (also known as a SYN Flood) or a UDP Flood, among several others.

3.3. Control Layer threats

Control Layer is mainly managed by SIP protocol. SIP uses clear text messages, meaning anyone with a computer and some programming knowledge can tap into a network and capture SIP messages. This is different from bit-oriented protocols like CCS7, which simply transport frames of bits that when grouped into a defined format can be decoded to specific messages and parameters. Since SIP uses clear text, if a hacker can capture these messages, that hacker is able to read subscribers' sensitive information such as their public and private identities. This information can then be used to "spoof" a subscriber. In other words, the hacker can use this information to gain access into the operator's network for his or her own use.

3.4. Application / Service Layer threats

Since applications are typically hosted on networked servers running conventional operating systems, they are vulnerable to the same type of threats as enterprise businesses experience. For example, a "Push-to-Talk" application running on a Linux-based server, or an Instant Messaging or VoIP Call Management application on a Windows-based server are all vulnerable to the same threats as their enterprise counterparts experience on a daily basis, such as a Denial of Service (DoS) intrusions, proliferation of viruses or worms that ultimately can impact uptime and cost carriers service revenue.

> **In mobile OS, generally there is a lack of appropriate permission control so as to ensure that other applications don't use VoLTE signalling network interface. This vulnerability can be exploited for free data access.**

4.0 Types of Attacks

There are many different forms of network breaches faced by IMS network for example; SIP signaling attacks, RTP media attacks and IP domain attacks. Some of the potential attacks that occur most often are summarized below.

4.1. Denial of Service (DoS) Attack

This attack floods P-CSCF and other IMS network elements with service requests. For example, in a REGISTER flooding attack, the attacker sends many REGISTER requests to the P-CSCF with fake or spoofed source addresses (e.g. SIP URI [uniform resource identifier]). In the case of distributed REGISTER flooding, the attacker generates multiple REGISTER requests with different spoofed and faked source addresses to overwhelm the IMS resources. It causes downfall of IMS resources and the legitimate users cannot get the services.

4.2. Eavesdropping

Hackers get session information if message are sent in clear text and can easily launch a variety of hijacking attack from session information. It may be registration hijacking or session hijacking. In registration hijacking attack, SIP REGISTER message is captured and the information contained therein is utilized to gain access to the network. To the network it appears as if the subscriber has changed locations in the network and sent a new registration request and a new location gets stored in the registrar. As a result of this, all subsequent session traffic for the legitimate subscriber are now sent to the hacker's destination instead of the subscriber's device. Similarly, a session hijacking attack is used to take over a session in progress.

4.3. SQL injection Attack

This is a type of message- tampering attack, which occur due to text based nature of SIP messages in IMS. This attack not only targets data modification but also causes DoS by collapse of database services. The utilization of a Web interface for the provision of value-added services makes IMS more vulnerable to this kind of attack. The SQL injection could be launched simply by inserting an SQL Statement when UE and P-CSCF start authentication procedures. When a malicious user tries to launch SQL injection in IMS, he or she spoof the SIP messages and inserts the malicious user SQL code in its authorization header. When P-CSCF receives a SIP message with an infected authorization header, It generates and executes the illegitimate SQL statement, which may delete data in the database. The existing solutions do not provide mitigation against this attack. The IMS also integrates the HTTP servlet container; therefore, an attacker can also utilize the HTTP message to launch the SQL injection attacks.

4.4. Media session termination Attack

The BYE request is used to terminate an established session. An attacker could utilize the BYE request to tear down a session. The attacker sends a fake BYE message, which is forwarded from P-CSCF to User A and it assumes that it is from User B, which wants to tear down the connection by sending the BYE message. As a result, User A stops the RTP flow immediately, while User B continues to send RTP packets to User A because User B has no notion that the connection should be terminated. To launch this kind of attack, the attacker needs to learn all necessary session parameters. This can be accomplished either by sniffing the network or performing a man-in-the-middle attack to insert a BYE request into the session.

4.5. CANCEL Attack

The CANCEL request terminates a pending INVITE request. The attacker could utilize the CANCEL method to cancel an INVITE request generated by a legitimate user. Before the final response is generated for an INVITE request, the attacker sends a fake CANCEL messages to the P-CSCF, which assumes that it is from a legitimate user. The IMS core acknowledges the CANCEL message and ceases the processing of the INVITE request.

4.6. Re-INVITE Attack

The INVITE request establishes a session or dialog between two user devices (UE). The objective of re-INVITE message is to modify the actual session information- for example, changing the addresses or ports, adding a media stream, or deleting a media stream . Therefore, the attacker could launch an attack by sending a forged re-INVITE message to modify the session.

4.7. IP multimedia services identity module (ISIM) cloning

This process changes the identity of one entity to that of an entity of the same type. The ISIM can be cloned by extracting the secret key (K) and international mobile subscriber identity (IMSI) from one ISIM and shifting to another ISIM using different attack techniques.

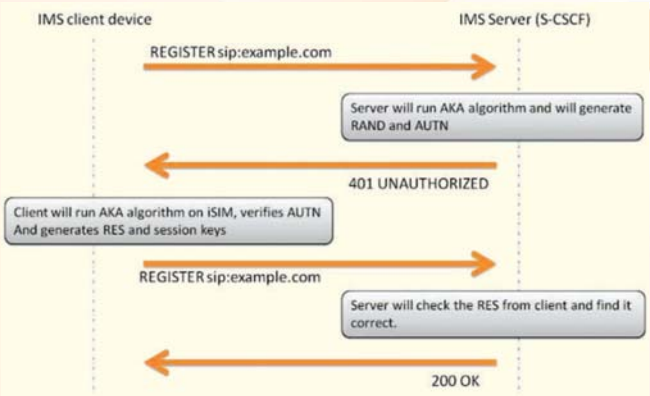
5.0 IMS Security mechanisms

5.1. Authentication Process in IMS

When a VoLTE client needs to connect to IMS network, it has to authenticate the network while network also needs to make sure that only the correct user is registered to its network. AKA Digest is one of the scheme to authenticate VoLTE client to the IMS server. AKA stands for "Authentication and key agreement". This scheme comes from the legacy 3gpp networks and has been widely used in LTE, 3G, CDMA and WiMAX technologies. In this mechanism, a secret key is already known to both user device (USIM, iSIM) and authentication servers (HSS, HLR).

The server will challenge the end user using AKA algorithms and shared key and sends a random RAND, AUTN values towards UE. UE will authenticate network and prepares result (RES for network to authenticate UE) with the help of shared key in UICC and parameters sent by Server. The step-by-step process is as follows:

- VoLTE Client sends SIP register request to IMS Server. The user is not authenticated at this point. The SIP register request contains IMS related identities.
- The IMS server (S-CSCF) obtains authentication vector from HSS, which contains a random challenge RAND, authentication token AUTN, expected authentication result XRES, a session key for integrity check IK, and a session key for encryption CK
- The server creates an authentication request, which contains the random challenge RAND, and the network authenticator token AUTN
- The authentication request is delivered to the client with "401 UNAUTHORIZED" message
- The client verifies the AUTN with the ISIM. If the verification is successful, the network has been authenticated. The client then produces an authentication response RES, using the shared secret K and the random challenge RAND.


IMS client device
IMS Server (S-CSCF)
REGISTER sip:example.com
Server will run AKA algorithm and will generate RAND and AUTN
401 UNAUTHORIZED
Client will run AKA algorithm on iSIM, verifies AUTN And generates RES and session keys
REGISTER sip:example.com
Server will check the RES from client and find it correct.
200 OK

3GPP AKA Operation in IMS

The authentication response RES is delivered to the server using new regiser sip message

- The server compares the authentication response RES with the expected response. If the two match, the user has been successfully authenticated
- Session keys IK and CK can be used for protecting further communications between the client and the server
- Server sends "200 OK" message to inform the VoLTE client about successful registration

5.2. Integrity protection of SIP signaling

IPsec ESP (Encapsulating Security Payload) provides integrity protection of SIP signaling between UE and the P-CSCF, protecting all SIP signaling messages at the IP level.

As a result of an authenticated registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF, all shared by TCP and UDP, is established in the P-CSCF and later in the UE. One SA pair is for traffic between a client port at the UE and a server port at the P-CSCF and the other SA is for traffic between a client port at the P-CSCF and a server port at the UE.

The integrity key IKESP is the same for the two pairs of simultaneously established SAs. The integrity key IKESP is obtained from the keying material established as a result of the AKA procedure, using a suitable key expansion function. This key expansion function depends on the ESP integrity algorithm. The integrity key expansion on the user side is done in the UE. The integrity key expansion on the network side is done in the P-CSCF.

5.3. Confidentiality protection of SIP signaling

If the local policy in P-CSCF requires the use of IMS specific confidentiality protection mechanism between UE and P-CSCF, IPsec ESP (Encapsulating Security Payload) provides confidentiality protection of SIP signaling between UE and the P-CSCF, protecting all SIP signaling messages at the IP level.

As a result of an authenticated registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF, all shared by TCP and UDP, is established in the P-CSCF and later in the UE. One SA pair is for traffic between a client port at the UE and a server port at the P-CSCF and the other SA is for traffic between a client port at the P-CSCF and a server port at the UE.

The encryption key CKESP is the same for the two pairs of simultaneously established SAs. The encryption key CKESP is obtained from the keying material established as a result of the AKA procedure, using a suitable key expansion function. This key expansion function depends on the ESP encryption algorithm. The encryption key expansion on the user side is done in the UE. The encryption key expansion on the network side is done in the P-CSCF.

5.4. SIP Security for CSCF interoperating with proxy located in a non-IMS network

SIP signalling protected by TLS specified in RFC 3261 may be used for protecting the SIP interoperation between an IMS

CSCF with a proxy/CSCF located in a foreign network. In this mechanism, SIP messages are sent over a Transport Layer Security-encrypted channel. Originally used for securing HTTP sessions, TLS can also be used to protect SIP session communications from eavesdropping or tampering. By deploying SIP-based devices that support Secure SIP, network administrators benefit from these increased levels of security for their IMS networks.

In a Secure SIP session, the SIP user agent client contacts the SIP proxy server requesting a TLS session. This SIP proxy server responds with a public certificate and the SIP user agent then validates the certificate. Then the SIP user agent and the SIP proxy server exchange session keys to encrypt or decrypt data for a given session. The SIP proxy server further contacts the next hop and similarly negotiates a TLS session, ensuring that SIP over TLS is used end-to-end.

TLS is a lighter-weight and easier to manage than IPsec, and thus more appropriate for SIP-based VoIP endpoints, which are often processing and resource constrained.

5.5. IMS media plane Security

The integrity and confidentiality protection for IMS media using RTP and RTCP is achieved by using the Secure Real-Time Transport Protocol (SRTP) and Secure RTCP protocol (SRTCP) defined in RFC 3711.

SRTP defines a profile of RTP, intended to provide encryption, message authentication, integrity and replay protection to the RTP data in both unicast and multicast applications. Since RTP is closely related to RTCP, which can be used to control the RTP session, SRTP also has a sister protocol, called Secure RTCP (or SRTCP); SRTCP provides the same security-related features to RTCP, as the ones provided by SRTP to RTP.

Utilization of SRTP or SRTCP is optional to the utilization of RTP or RTCP; but even if SRTP/SRTCP are used, all provided features (such as encryption and authentication) are optional and can be separately enabled or disabled. The only exception is the message authentication feature which is indispensably required when using SRTCP.

For encryption and decryption of the data flow and hence for providing confidentiality of the data flow, SRTP (together with SRTCP) utilizes AES as the default cipher.

Encryption algorithms do not secure message integrity themselves, allowing the attacker to either forge the data or at least to replay previously transmitted data. Hence the SRTP standard also provides the means to secure the integrity of data and safety from replay.

To authenticate the message and protect its integrity, the HMAC-SHA1 algorithm (defined in RFC 2104) is used. The HMAC is calculated over the packet payload and material from the packet header, including the packet sequence number. To protect against replay attacks, the receiver maintains the indices of previously received messages, compares them with the index of each new received message and admits the new message only if it has not been played before. Such an approach heavily relies on the integrity protection being enabled to make it impossible to spoof message indices.

5.6. Session Border Controller (SBC)

SBCs can provide security and protection against unauthorized access into the trusted network, invalid or malicious calls including Denial of Service (DoS) attacks and bandwidth theft by authorized users.

To provide this security, the SBC

- identifies and authenticates each user and determines the priority of each call
- limits call rates and resource usage to prevent overloads
- authorizes each media flow and classifies and routes the data to ensure suitable QoS
- prevents unauthorized access for both signaling and media traffic.

SBC also helps in maintaining privacy. An SBC can be used to remove confidential information from messages before they leave the core network, including details of internal network topology and routing of signaling through the core network. It can also hide the information about a user that the user does not wish to be made public.

6.0 Conclusion

The open and distributed architecture of IMS offers the advantage of flexibility in implementation and deployment, but at the same time creates a multitude of interface points that must be secured. It presents significant security challenges that must be addressed by the carriers as IMS moves into widespread deployment. Security threats in any network cannot be eliminated completely. However, by adopting innovative and powerful security counter-measures these threats can be mitigated to a great extent. These counter-measures include identifying vulnerabilities, adopting a strategy to take care of these vulnerabilities and putting in place a powerful architecture which is secure enough to defeat the threats and minimise the risk.

REFERENCES

i. 3GPP TS 33.203 version 11.2.0 Release 11 Access security for IP-based services

ii. White Paper on "IMS Architecture - The LTE User Equipment Perspective" by SPIRENT.

iii. "IMSecure – Attacking VoLTE" by ERNW

iv. "IP MULTIMEDIA SUBSYSTEM (IMS) SECURITY MODEL" International Journal of Advance Research, Volume 1, Issue 3, March 2013

v. "Securing IP Multimedia Subsystem with the appropriate Security Gateway and IPSec Tunneling", Journal of Security Engineering 2011

vi. STRENGTHENING SECURITY OF IP MULTIMEDIA SUBSYSTEM, Nauris Paulins, Latvia University of agriculture

Mandatory Testing and Certification of the Telecom Equipments (MTCTE)

The Mandatory Testing and Certification of the Telecom Equipments (MTCTE) scheme has been notified on 5thSeptember 2017 and comes into effect from 1st October 2018. Under the scheme, all telecom equipments, whether imported or indigenously manufactured, are to be tested and certified against Essential Requirements (ERs) notified by Telecom Engineering centre (TEC). Copies of Gazette notification and the MTCTE scheme are available at TEC website.

Most of the countries specify minimum technical regulations for telecom products before importation in their country and induction in their network. Though India is the second largest market of telecom equipments, until date, India was not having such a framework to regulate domestic as well as imported products. The Government of India is committed to follow international best practices and introduction of MTCTE is a move in the right direction. Global best practices have been included in the MTCTE scheme, with due regard to Indian requirements and regulations. TEC, which already has vast experience in formulation of Generic Requirements (GRs) and Interface Requirements (IRs), has taken up the task of framing of ERs along with Security Assurance unit of DoT against which the telecom equipments need to be tested for conformity and certified. A consultative mechanism through Mandatory Testing Consultative Forum (MaTCoF) has been prescribed for consultation with stakeholders before finalization of ERs. The finalised ERs are being progressively published on TEC website.

The MTCTE procedure itself was developed after series of consultations with stakeholders, which include Telecom Service Providers and Original Equipment's Manufacturers (OEMs). The concerns raised by them during several rounds of consultations including open forum conference on have suitably been addressed while framing the scheme. Two very important and useful feedback, amongst others, given by stakeholders was (i) to introduce an online system to avoid manual intervention, and (ii) to permit suitable transition time, of at least one year. Accordingly, the mandatory certification, notified on 5th September 2017, has been made applicable with effect from 1.10.2018. Further, the testing and certification process under MTCTE like application, registration, evaluation and certification will be administered through an online portal, being developed for this purpose, which will reduce human intervention and make the whole process efficient and transparent.

Under the scheme, test results from Indian accredited labs designated by TEC, called Conformity Assessment Bodies (CABs) are to be submitted. Alternatively, test results from designated labs of MRA partner countries are also accepted. TEC has notified an amended scheme of designation of labs and large number of labs including many from government organisations and academic institutions have shown interest in becoming CAB. While Indian labs are progressively being designated, in order to meet the demand in the initial phases of implementation of MTCTE, test results from any lab accredited under ILAC network shall be accepted as a relaxation, until 31st Match 2019.

In order to ensure that the provisions of the scheme support and not decelerate manufacture and import of telecom equipments, TEC has adopted a continuous process of industry consultation. While industry representatives had been interacting with TEC through MaTCoFs, open forum consultations have also been carried out. In the latest consultative meeting held on 16th March 2018, it emerged that certain concerns required focussed attention. Accordingly, six focussed areas were identified. The meeting of focussed area related to custom clearance and export and import related issues was held on 11th April 2018, wherein representative from Customs was also present. This helped in clarifying majority of the issues of concern immediately, and a few issues requiring some action were identified, which shall be resolved separately. Another meeting of focussed area related to labelling of products and defining procedure for inclusion of associated models in same certificate was held on 12th April 2018. The issues remaining unresolved in this meeting will be taken up in next meeting on this topic. In addition, separate meetings of focussed areas covering issues related to testing of IoT devices, and those related to testing of IT and software intensive products are planned. Beta version of MTCTE online portal is also expected to be launched soon.

Through the MTCTE scheme, TEC is committed to implement the international best practice of mandatory testing and certification of telecom equipments in a most transparent manner, to ensure safety of user, safety of equipment and environment, and safety of citizen and country, while ensuring that the ongoing pace of development and advancement in telecom field is not adversely affected.

Visit http://www.tec.gov.in/certification-approval-procedure/ or contact ddgtc.tec@gov.in.

Activities at NTIPRIT (JAN-18 to MAR-18)

1. **National Telecommunications Institute for Policy Research, Innovations & Training (NTIPRIT)**

   The Department of Telecommunications established the National Telecommunications Academy (NTA) in the year 2010 as the technical training institute of the department. Subsequently, in year 2011, the mandate of institute was expanded by bringing into the activities related to Policy Research and Innovations under its ambit and the institute was rechristened as National Telecommunications Institute for Policy Research, Innovations & Training (NTIPRIT). Since then NTIPRIT has grown from strength to strength and the institute is now a Central Training Institute (CTI) enlisted with Department of Personnel & Training. NTIPRIT is presently operating from the ALT campus at Ghaziabad.

2. **Presentation by ITS-2015 batch officer trainees (OTs), before Hon'ble Minister of State Communications (IC)**

   Hon'ble Minister of State for Communications (IC), Sh. Manoj Sinha had desired that Officer Trainees of ITS-2015 batch shall study different policies and procedures of DOT during their field attachments, identify problems and suggest solutions. 33 OTs were divided in 11 groups with 3 OTs each and each group selected a topic for presentation to Hon'ble Minister. In this regard, Officer Trainees were called by Hon'ble Minister of Communications on 13.03.2018 for presentation. Topics of presentations are as below;

   (a) e-KYC based Customer verification

   (b) DBT connectivity issues and public grievances

   (c) Wi-fi calling using BBNL broadband N/W for improving rural connectivity

   (d) Grey market analysis

   (e) Verification of new mobile subscribers

   (f) OSP Registration and Regulations

Hon'ble Minister of Communications is welcomed by Sr. DDG (TEC/NTIPRIT)

Hon'ble Minister and other dignitaries listening to presentations from Officer Trainees

   (g) CMS implementation

   (h) Optimization opportunity and Security issues in Satellite Communication in Andman & Nicobar

   (i) Telecom connectivity constraints in North East

   (j) Utilization of optical fiber and installation of BTS in Bharatnet covered villages

   (k) Teledensity in rural areas: Challenges & way forward

   During the event, Special Secretary, Member (T), DG Telecom, Sr. DDG (TEC/ NTIPRIT), DDG (Training) DoT and DDG (Training), NTIPRIT, Director (Training) and other Senior officers were also present.

Officer Trainees of Indian Telecom Service-2015 batch, presenting before Hon'ble Minister

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

   i. ITS-2014 batch (4 officers)

   ii. ITS-2015 batch (34 officers)

   iii. ITS-2016 batch (34 officers)

   iv BWS-2013 batch (1 officer)

v. BWS-2015 batch (1 officer)

vi. BWS-2016 batch (3 officers)

vii. JTO-2015 Batch (3 officers)

viii. JTO-2016 Batch (2 officers)

Various training programs like technical modules and DoT, TEC attachment for ITS/BWS/JTO were conducted during this period as per respective training calendar.

Training Courses conducted by NTIPRIT during the year 2017-18

Sl. No.	Type of Courses	No. of Courses Conducted	No. of persons trained	No. of Trainee days
1	Induction Training of ITS & BWS Group-A officers	75	81	14192
2.	Induction Training of JTOs Group-B officers	16	23	1777
3.	In-service courses for officers of DoT	4	-	129
4.	Workshops/Seminar	-	-	129
	Total	**95**	**104**	**16098**

(Apart from classroom training, Induction training also includes attachment to various units of DoT)

हिंदी कार्यशाला

दूरसंचार अभियांत्रिकी केंद्र में दिनांक 15.03.2018 को एक हिंदी कार्यशाला का आयोजन किया गया। इस कार्यशाला में कुल 19 अधिकारियों/कर्मचारियों ने भाग लिया। इस कार्यशाला में अतिथि वक्ता के रूप में श्री नगेन्द्र सिंह, वरिष्ठ तकनीकी निदेशक (राजभाषा विभाग) ने भाग लिया। उन्होंने यूनिकोड इन्स्टाल करने, गूगल–ट्रांसलेसन, गूगल वॉइस टाइपिंग, क्रोम ब्राउजर का प्रयोग करके हिंदी/अंग्रेजी में डिक्टेशन देने और गूगल डॉक्स पर कार्य करने के बारे में विस्तार से उल्लेख किया। श्री नगेन्द्र सिंह द्वारा कार्यालय कार्यों में हिंदी का ज्यादा से ज्यादा प्रयोग करने आदि के बारे में विस्तार से बताया गया तथा हिंदी के बारे में काफी रोचक एवं ज्ञानवर्धक जानकारियाँ उपलब्ध कराई गई।

हिंदी कार्यशाला में उपस्थित अधिकारी एवं कर्मचारी

Approvals from JAN-18 to MAR-18

Sl. No.	Name of the Manufacturer/Trader & Name of Product & Model No.
A	Sunren Technical Solutions Pvt Ltd
1	Group 3 Fax Machine/Card, LEX-M14-002
2	Group 3 Fax Machine/Card, VCVRA 1710
B	Sunrise Corrugated (India) Pvt Ltd
3	Double Walled Corrugated HDPE Ducts (DWC), DWC HDPE 110 mm dia
C	Matrix Comsec Pvt Ltd
4	PABX for Network Connectivity, Eternity PE 6S
5	PABX for Network Connectivity, Eternity MENX
D	Nx Value Solutions India Pvt Ltd
6	Interchange Of STM-1, STM-4, STM-16, STM-64& STM-256 Signals, Mediant STM
7	PABX For Network Connectivity, Sonus SBC2000
8	Group3 Fax Machine/Card, LEX-M03-02
9	Group3 Fax Machine/Card, BOISB-1500-03
10	Group3 Fax Machine/Card, BOISB-1102-03
11	Terminals For Connecting to PSTN, Converge Pro 2 (128T)
12	Terminals For Connecting to PSTN, Converge Pro 2 (48T)

Important Activities of TEC during JAN 18 to MAR 18

GRs/IRs issued:

- GR on IP-DSLAM
- GR on IVRS
- GR on very high speed digital subscriber line (VDSL & VDSL2) equipment for remote terminal applications
- GR on ADSL2+ system for remote applications
- IR on Interchange of STM-1, STM-16, STM-64 and STM-256 signals between different networks

MATCOF meetings conducted for:

- Various Mandatory Testing Consultative Forum meetings were conducted for formulation of Essential Requirements for different types of products & their variants in TEC

DCC meeting conducted for:

- GR on NFVI+VIM
- GR on Unified Threat Management
- GR on Ethernet to E1 converter
- IR on Mobile Radio Trunking communication equipment
- IR on Mobile Radio Trunking Subscriber Unit
- Test Procedure for Measurement of Electromagnetic fields from Base station antenna

Sub DCC meeting conducted for:

- GR on Session Border Controller
- IR on Session Border Controller

Study/white paper issued:

- WLAN Security
- IMS Security
- Application Security

Representation of TEC in Training/Seminar/Meetings:

- ITU-T TSAG & SG-20 Meeting at Geneva, Switzerland
- International Conference on Disaster manager at NDMA, New Delhi
- Training on Cyber Security at NEC, New Delhi
- High level forum of spectrum group at IIT Bombay

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 NWG-20 in TEC
- 04 new Labs have been designated as CAB of TEC (M/s The Tata Power Company Limited, Strategic Engineering Division, Bengaluru, M/s Classic Instrumentation Pvt. Ltd., Noida, M/s Electronic Test & Development Centre, Bengaluru and M/s React Laboratories, Bangalore)
- Draft recommendation ITU-T "X.SAMTN" has been approved in SG-17 meeting held in Geneva, Switzerland.
- Technical presentations on "Test Cases of RFCs & its testing" was given by M/s IXIA Ltd. in TEC.
- Technology Approval for CDOT GPON system completed.

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
अप्रैल 2018 : खुर्शीद लाल भवन
भाग 22 : जनपथ
अंक 2 : 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