भाग 23 / अंक 1 जनवरी 2019 त्रैमासिक पत्रिका

ISO 9001 : 2008
TEC
दूरसंचार अभियांत्रिकी केन्द्र
TELECOMMUNICATION ENGINEERING CENTRE

टी ई सी संचारिका
NEWSLETTER

Conference on M2M/IoT Enabling Smart Infrastructure

A one day "Conference on M2M/ IOT Enabling Smart Infrastructure" was inaugurated by Shri Manoj Sinha, Hon'ble MoSC(IC) in TEC on 8th Jan, 2019. Ms. Aruna Sundararajan, Secretary (Telecom) & Chairman, Digital Communications Commission, Shri Ravi Kant, Member(Services), Shri D. Manna, DG Telecom and other dignitaries from DOT, USOF, TRAI, TDSAT, CDOT, MTNL, BSNL, BBNL, TCIL, TSDSI, Industry and academia participated in the conference.

During the inaugural session of the conference, two TEC Technical Reports were released by Hon'ble Minister of State for Communications (IC) on "*Design & Planning of Smart Cities by using IOT/ICT*" and "*Recommendations for IOT/ M2M Security*". These reports will be useful to all stakeholders i.e. Planners, Policy makers, Manufacturers and Academia and serve as guiding tool.

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastructure
&
Release of Technical Repo n M2M/IoT
Inauguration by
Shri Manoj
अरुणा सुंदरराजन
मनोज सिन्हा
रवि कान्त
डी. मन्ना

Release of Technical Reports on M2M/IoT by Shri Manoj Sinha Ji, Hon'ble MOSC (IC) & MOS Railways

Continue from cover page......

Inauguration of 'MANAK' conference room by Hon'ble MOSC (IC)

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastr
Release of Technical
on M2M/IoT
Shri Shiwa

Welecome of Shri Manoj Sinha, Hon'ble MOSC (IC) by Shri Mahabir Prashad Singhal, Sr. DDG, TEC

Welecome of Ms. Aruna Sundararajan Secretary(T), DoT, by Shri Mahabir Prashad Singhal, Sr. DDG, TEC

"Technology Approval" was granted to CDOT for indigenously developed Wi-Fi Access Point, which will be manufactured by CDOT's Transfer-of-Technology partners in India. It will give a big boost to Make-in-India Programme of Government.

An MoU was also signed between TEC and CSIR-CEERI, Pilani on 08.01.2019 and exchanged in the presence on Honourable MOSC(IC) Shi Manoj Sinha and other dignitaries during the inaugural session of the conference. It will promote collaboration between TEC and the research institutes in the area of development of standards for Future Telecom & ICT Technologies.

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastructure
Release of Technical Reports on M2M/IoT
Shri Manoj Sinha
Ms. Aruna Sundararajan

MoU between TEC & TCIL: Ms. Deepa Tyagi, DDG(FN), TEC, New Delhi and Shri (Prof) Raj Singh, Director, CEERI, Pilani exchanging the same

The inaugural session was followed by technical sessions on M2M/IoT which were held during the conference. The technical sessions had speakers from TEC and the industry. The audience had officers from DOT, TEC, NTIPRIT, CDOT, MTNL, BSNL, CSIR-CEERI and the industry, who keenly heard the speakers and later on interacted with them during question & answer sessions. The details of the technical sessions are given below:

(a) Shri Sushil Kumar, DDG(IoT), TEC briefed the audience on the M2M/ IoT technology and the works done in TEC.

(b) 1st Technical Session on "IoT Enabling Smart Verticals - Use Cases & Technologies".

(c) 2nd Technical Session on "Smart Cities design and planning with IoT & ICT".

(d) 3rd Technical Session on "M2M / IoT Standardization & its role in Smart Cities".

(e) 4th Technical Session on "Security Challenges and Testing & Certification of Smart Devices/ Equipment".

Telecom News: At a Glance

1. 'MTCTE Portal' to administer the Mandatory Testing & Certification of Telecom equipment and 'SARAL SANCHAR' for processing of applications for provision of license & registration of telecom services was launched by Hon'ble MOSC(IC) Shri Manoj Sinha ji on 15-11-2018 in a function at Bengaluru.
2. Hon'ble MOSC(IC) inaugurated the Security Assurance Standards Facility of the National Centre for Communications Security of an event held in Bengaluru on 15-11-2018. This is the first security lab in India.
3. India Mobile Congress 2018 (IMC-2018) was organised by DoT & COAI in OCT-2018 in New Delhi.
4. DoT has issued National Frequency Allocation Plan - 2018 in Nov, 2018.

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastructure

Speakers in Session of IoT enabling Smart Verticals - use cases & technologies

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastructure
&
Release of Technical Reports on M2M/IoT
Inauguration by
Shri Manoj Sinha
Guest of Honour
Ms. Aruna Sund ian

Speakers in Session of Smart Cities design and planning with IoT & ICT

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastructure

Speakers in Session of Security Challenges and Testing & Certification of Smart devices / equipment

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastructure

Speakers in Session of M2M / IoT Standardization & its role in Smart Cities

Key Recommendations from the Technical Report- Design and Planning Smart Cities with IoT/ ICT

1. Cities should use available resources - smartphone-based sensor-networks as well as crowdsourced data from its citizens to enrich its services were possible.
2. The different city services should break walls and share data. Common service principles/common service layer and open data concepts should be adopted by Cities.
3. Smart City planners should employ Design, Systems and Future thinking frameworks to conceptualize, design and develop solutions using IoT that are long lasting and resilient.
4. Society 5.0, a super smart nation with digitalization across all levels of society, to positively transform India is what we should work towards.
5. There is a need for proper town planning using GIS for efficiently deploying various solutions such as traffic management, street light, waste management etc.

Article on IOT – M2M security

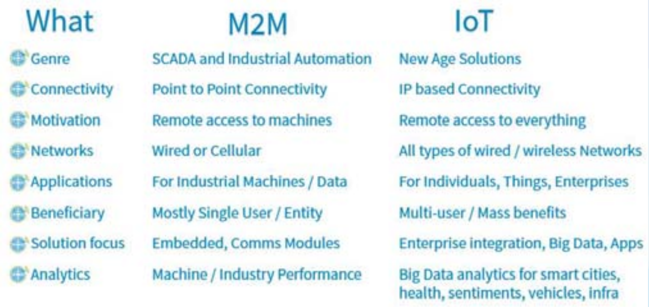
1.0 M2M (Machine to Machine communication)

M2M communication refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. M2M uses a device (such as a sensor or meter) to capture an event, which is relayed through a network (wireless, wired or hybrid) to an application, that translates the captured event into meaningful information.

2.0 Internet of Things

A global infrastructure for the information society, enabling advanced services by interconnecting things (physical and virtual) based on existing and evolving interoperable information and communication technologies.

3.0 How is IoT different from M2M?



What	M2M	IoT
Genre	SCADA and Industrial Automation	New Age Solutions
Connectivity	Point to Point Connectivity	IP based Connectivity
Motivation	Remote access to machines	Remote access to everything
Networks	Wired or Cellular	All types of wired / wireless Networks
Applications	For Industrial Machines / Data	For Individuals, Things, Enterprises
Beneficiary	Mostly Single User / Entity	Multi-user / Mass benefits
Solution focus	Embedded, Comms Modules	Enterprise integration, Big Data, Apps
Analytics	Machine / Industry Performance	Big Data analytics for smart cities, health, sentiments, vehicles, infra

4.0 IOT Security may be defined as:

"IoT security deals with safeguarding connected devices, physical and virtual, in addition to the networks and IT security, for the Internet of things "

Whilst many service providers, such as those in automotive, healthcare, consumer electronics and municipal services, may see their particular security requirements as being unique to their market, this is generally not the case. Almost all IoT services are built using endpoint device and service platform components that contain similar technologies to many other communications, computing and IT solutions. In addition to this, the threats these different services face, and the potential solutions to mitigate these threats, are usually very similar, even if the attacker's motivation and the impact of successful security breaches may vary.

5.0 Functional Architecture and Domains:

The IoT / M2M solution can also be appreciated from a geographical lens as depicted in Figure 1. Sensors, Devices and Gateways are usually the dispersed nodes, found in the field and customer premises. Networks vary in scale from small areas and neighbourhoods to cities, states and country wide networks. Applications and Services are mostly delivered from Data Centres and Clouds, centralised in a few places. Trust frameworks are all pervasive; these are embedded into Field Nodes, Communication Networks, Applications and Services.

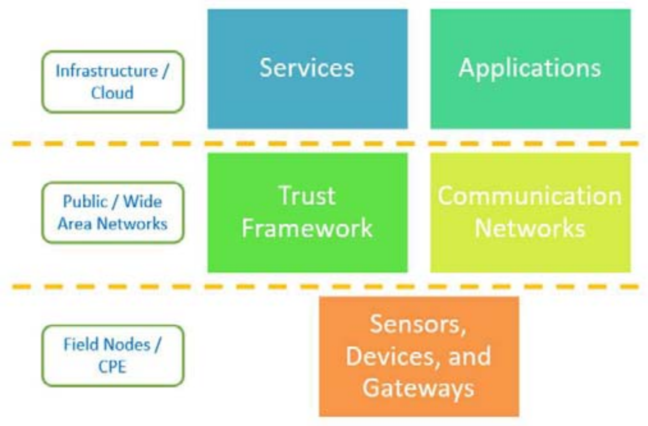


Figure 1 : Functional View

6.0 Security Threats, Challenges, Risks and Securing IOT/M2M Ecosystem:

Security is one of the most important considerations while designing an M2M system, in order to prevent the hackers to break into M2M applications designed to control, for example, building security, environmental monitoring, vehicle tracking, etc. In order to prevent possible security violations, the most appropriate communication techniques must be used, because different types of communication techniques present different encryption and security features.

The future of IoT/M2M cannot be realized without addressing security and privacy risks and policy issues. Securing and protecting the things that matter most—our systems, our data, and our privacy—is a shared responsibility. Security and privacy must become part of every product's feature set.

6.1 IoT/M2M Security Threats

The Following stakeholders are affected by the IoT/M2M Security threats

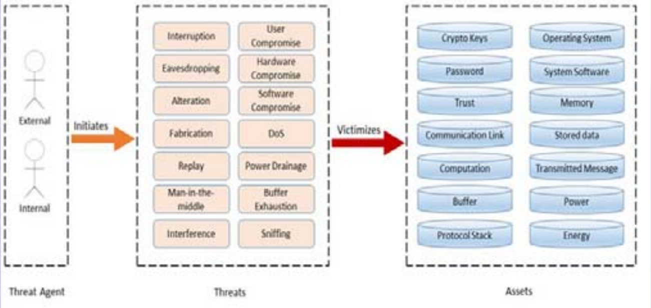
- M2M Application Service Provider;
- Manufacturer of M2M Devices and/or M2M Gateways;
- M2M Device/Gateway Management entities;
- M2M Service Provider;

- Network Operator
- User/Consumer

6.1.1 Understanding the potential threats in IoT/M2M environment

In a completely closed network, like in a verticalized captive use case, security risks are minimal. But, as M2M embedded systems become IP-enabled and interconnected the attack surface becomes open to threats. Services provided by the IOT/M2M System to IOT/M2M applications establish the need for trusted security credentials to secure connections between applicative entities, including the other involved functions. IoT security requires a nuanced understanding of its unique characteristics.

An understanding of the potential threats in the IoT environment has been broadly shown in the (Figure 2) diagram below, whereby various internal/external threat agents initiating threat by virtue of interruption, eavesdropping, buffer exhaustion, software/hardware compromise etc. which victimizes the various assets (like memory, crypto keys, buffer, power, energy etc.) and may cause malfunctioning of these assets.



Source: http://secret.cis.uab.edu/research/iot-security/

Figure 2: Potential threats in IoT

IoT opens a completely new dimension to security. The IoT is where the Internet meets the physical world. This has some serious implications on security as the attack threat moves from manipulating information to controlling actuation (in other words, moving from the digital to the physical world). Consequently, it drastically expands the attack surface from known threats and known devices, to additional security threats of new devices, protocols, and workflows. Many operational systems are moving from closed systems into IP based systems which further expands the attack surface.

For the most part, machines are unattended devices. People hesitate in adding security features like proactive monitoring as this could slow down performance and therefore at times the designers may have ignored security issues, in turn leaving devices vulnerable. The same also applies to embedded systems as CPU, battery life and memory all take priority and design choices are often made that favour speed of roll out over security. The inclusion of security component, such as cryptography, can slow communications and performance, impact and eat into processing capability of the device working on a very low power long term battery to sustain or survive.

6.1.2 Frauds and attacks in IOT/M2M systems

Most commonly, an attacker installs unauthorized IOT/M2M service-layer software and/or modifies authorized software functions in IOT/M2M Devices or IOT/M2M Gateways. This attack may be used to:

i. commit fraud, e.g. by the incorrect reporting of energy consumption;

ii. cause a breach of privacy by obtaining and reporting confidential information to the attacker

iii. cause the disclosure of sensitive data such as cryptographic keys or other credentials

iv. prevent operation of the affected IOT/M2M Devices/Gateways

6.2 Challenges in IoT/M2M Security

IoT security challenges can broadly be depicted by the Figure 3 below showing security challenges in various aspects of IoT such as authentication, confidentiality, privacy, access control etc.

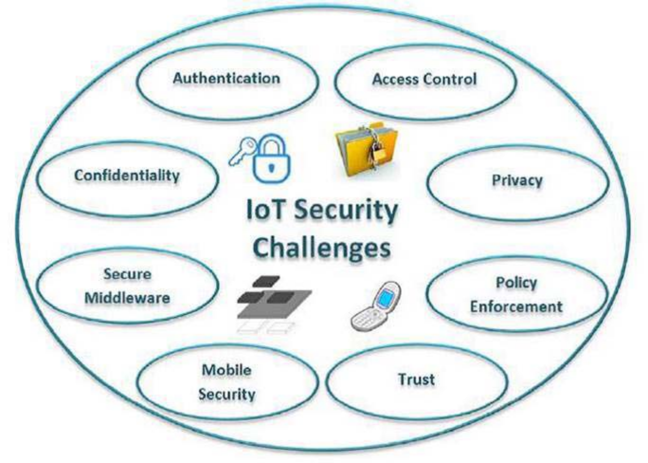


Figure 3 : IoT Security Challenges

6.2.1 Challenges - Security of Embedded Systems

In addition to the unique risks for M2M systems, embedded systems in general contain inherent security risks. These include: Firmware: The majority of software running on embedded systems is firmware, which can be easily changed, maliciously altered and then uploaded—replacing the authentic file. Anti-tampering techniques when creating the firmware and the use of application whitelisting on devices in the field protect firmware from exploitation.

Many of the embedded systems in place today are unlikely to be connected to a network 100 percent of the time. Inconsistent or intermittent network connectivity increases the chances of a device connecting to an unsecured network. If an embedded system is online only occasionally, it is more likely to be dependent on a single node for network access, which creates a single point of failure or attack. Additionally, devices with only occasional connectivity are more difficult to monitor for issues and more difficult to troubleshoot and upgrade.

In some cases, physical access to embedded devices is necessary for maintenance and upgrades. However, embedded devices that require or are open to physical access are exposed to two security threats.

1. First, it is more difficult to keep these systems up-to-date because they require human intervention. The time and expense involved may be prohibitive.
2. Second, the physical presence of an adversary is a concern because these devices can be exchanged or tampered with or used to introduce false information into the system to cause a direct failure.

Unencrypted Data: As often occurs in M2M devices, data encryption is omitted from embedded systems. With access to any particular end point or data point, it is not difficult to put a sniffer on that network, intercept network traffic over a variety of different protocols, and figure out how to exploit that information.

6.2.2 Challenges - Security

A major disruption of the traditional model for the new brings its own set of challenges few of them are listed below:

(i) Typically small, inexpensive devices with little or no physical security.

(ii) Though inexpensive, every device still has to compute something and also have some security feature. Also, it should not add to latency in processing.

(iii) Computing platforms, constrained in memory and compute resources, may not support complex and evolving security algorithms due to the following factors:

- o Limited security compute capabilities.
- o Encryption algorithms need higher processing power
- o Low CPU cycles vs. effective encryption

(iv) Designed to operate autonomously in the field with no backup connectivity, if primary connection is lost.

(v) Mostly installed prior to network availability which increases the overall onboarding time.

(vi) Requires secure remote management, up-dating during and after onboarding.

(vii) Scalability and management of billions of entities in the IoT ecosystem.

(viii) Identification of endpoints in a scalable manner, Sometimes the location may be more important than the individual identifier (ID).

(ix) Management of Multi-Party Networks.

(x) Crypto Resilience

- o Embedded devices may outlive algorithm lifetime.
- o Crypto algorithms have a limited lifetime before they are broken

(xi) Physical Protection

- o Mobile devices can be stolen
- o Fixed devices can be moved

(xii) Tamper Detection techniques and design

- o Always On: High Poll rate, more energy, quick detection.
- o Periodic Poll: Less energy, slower detection
- o On-event Push: Minimal energy, no detection

6.2.3 Challenges - Authentication and Authorization

The IoT entities will generally not be a single use, single ownership solution. Consequently, Authentication and Authorization of M2M devices in a dynamic and autonomous world will pose serious research challenges.

6.2.3.1 Authentication

Since not all communications protocols are capable of mutual authentication, or have strong cryptography, it is imperative that the application entities in the value chain design a sufficient protocol that enforces confidentiality and integrity, rather than relying on the communications protocol. Even more robust protocols that incorporate mutual authentication, such as LTE, do not address the security of the infrastructure beyond the cellular communications network. Only higher layer protocol security can address the risk of weaknesses in infrastructure beyond the control of the cellular carrier.

At the heart of IOT secure framework is the authentication layer, used to provide and verify the identify information of an IoT entity. When connected IoT/M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device. The way to store and present identity information may be substantially different for the IoT devices. Note that in typical enterprise networks, the endpoints may be identified by a human credential (e.g., username and password, token or biometrics).

The IoT/M2M endpoints must be fingerprinted by means that do not require human interaction. Such identifiers include radiofrequency identification (RFID), shared secret key, X.509 certificates, the MAC address of the endpoint, or some type of immutable hardware-based root of trust. Establishing identity through X.509 certificates provides a strong authentication system. However, in the IoT domain, many devices may not have enough memory to store a certificate or may not even have the required CPU power to execute the cryptographic operations of validating the X.509 certificates (or any type of public key operation).

Existing identity footprints such as 802.1ar and authentication protocols as defined by IEEE 802.1x can be leveraged for those devices that can manage both the CPU load and memory to store strong credentials. However, the challenges of the new form factors, as well as new modalities, create the opportunity for further research in defining smaller footprint credential types and less compute intensive cryptographic constructs and authentication protocols.

6.2.3.2 Authorization

The second layer of this framework is authorization that controls a device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity. With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information. For example, a car may establish a trust alliance with another car from the same vendor.

That trust relationship, however, may only allow cars to exchange their safety capabilities. When a trusted alliance is established between the same car and its dealer's network, the car may be allowed to share additional information such as its odometer reading, last maintenance record, etc. Fortunately, current policy mechanisms to both manage and control access to consumer and enterprise networks map extremely well to the IoT/M2M needs. The big challenge will be to build an architecture that can scale to handle billions of IoT/M2M devices with varying trust relationships in the fabric.

All India Heads of Police Communication Conference on 'Modernization of Police Communication and Challenges thereof'

A Conference was organized by Directorate of Coordination Police Wireless (DCPW) at Vigyan Bhawan, New Delhi on 19th & 20th Nov, 2018 which was inaugurated by the Minister of State for Communications (IC) and Minister of State for Railways, Shri Manoj Sinha Ji. A keynote address was given by Shri Mahabir Prashad Singhal, Sr. DDG, TEC on 20th Nov, 2018. Shri Sushil Kumar, DDG(IoT) also gave a presentation in the conference.

समन्वय निदेशालय पुलिस बेतार
Directorate of Coordination Police Wireless
गृह मंत्रालय, भारत सरकार
Ministry of Home Affairs, Government of India
All India Heads of Police Communication Conference
Modernisation of Police Communication and Challenges thereof

Addressing the session by Sr. DDG, TEC

6.2.4 Challenges - Heterogeneity and Resource Constraints

Given the limitations on the computational capabilities of many sensing and actuating platforms, security technologies must be developed to cope with and supported by architectures with the characteristics similar to the ETSI M2M architecture. For example, applications using passive Radio-Frequency Identification (RFID) tags are unable to support security mechanisms requiring the exchange of many messages and communication with servers on a network domain.

Lightweight solutions for symmetric and asymmetric cryptography which have been proposed in recent years provide a useful guidance in this context. The heterogeneity of sensing/actuating M2M devices may also be addressed by security approaches at higher layers of the protocol stack or at the middleware, in line with the approach previously discussed regarding Identification, authentication, authorization and trust.

6.2.5 Challenges - Privacy and its Preservation

Privacy is one of key importance nowadays. People are concerned about their personal data that is on the internet. Privacy can be divided into a few categories that have unique technical aspects:

(i) Communication privacy
(ii) Position privacy (Location privacy)
(iii) Path privacy
(iv) Identity privacy (Personal privacy)
(v) Personal data (use crypto for data protection)

Sticky policies are a way to cryptographically associate policies to encrypted (personal) data. These policies function as a gate keeper to the data. The data is only accessible when the stated policy is honoured. System keeps track of personal data relating to the user, as well as applied policies and service customizations.

For some M2M applications (in the context of the IoT) the user will require to be able to control the amount of personal information exposed to third parties, for instance in maintaining privacy while exposing personal records in healthcare applications. On the other end, other M2M applications may require that some of that information is available in case of necessity, for instance with M2M vehicular applications in case of traffic accidents.

Privacy Preservation

Preservation of privacy has been a concern since the dawn of the Internet. IoT will exacerbate the problem because many applications generate traceable signatures of the location and behaviour of the individuals. Privacy issues are particularly relevant in healthcare, and there are many interesting healthcare applications that fall within the realm of IoT. In this environment, it is essential to verify device ownership and the owner's identity while decoupling the device from the owner. Shadowing is a mechanism that has been proposed to achieve this.

Security and privacy

The various challenges posed to the addressing of security in M2M may benefit from a paradigm shift in how the various security requirements are guaranteed. For example, scenarios without a security infrastructure in place may consider classic security solutions side-by-side with new decentralized and distributed approaches. As in other scenarios M2M systems may be unable to derive definitive conclusions about the identity or intents of other devices, security mechanisms may need to consider compromises between the enforcement of definitive security controls and the acceptance of controlled risks.

6.2.6 Challenges – Identity, Anonymity and Liability

M2M Connectivity requires that the user and the use case be identified. Anonymity is necessary as applications may only be accepted if the user is guaranteed to have a certain degree of protection of its personal (or other) information. Liability is a deeply related requirement, as other applications may require access to private information in case of necessity, for example for legal purposes. As anonymity will be required in M2M, research can target the applicability of light weighted formal anonymity models such as k-anonymity to M2M environments.

Possible alternative approaches are the development of mechanisms for data transformation and randomization. Intrusion detection will also be relevant for autonomous M2M environments. Autonomous and cooperative methods allowing the early detection of node compromises may be the path to follow in this domain.

7.0 Securing IOT/M2M

Implementing security features and countermeasures to threats requires mechanisms that provide security related operations with an appropriate level of confidence. Sensitive functions are typically performed in termination points within the M2M System. Examples of sensitive functions include:

(i) cryptographic algorithms (session) key derivation functions
(ii) hash functions

In general, cryptographic functions operate on inputs such as messages and keys, and produce outputs such as cipher texts and signatures. Public key encryption relies on a pair of related keys, one secret and one public, associated with each individual participating in a communication. While slower than secret key cryptography, public key systems are preferable when dealing with networks of devices that need to be reconfigured fairly often.

A detailed risk assessment/evaluation of the level of impact of the threat depends on the assets and their value. The security affected in the various domains includes:

(i) Application domain security;
(ii) Intra Common Services domain security;
(iii) Inter Common Services domain security;
(iv) Underlying Network security, if keys are shared with underlying network.

8.0 Address Security Early: Threat Modelling

Securing an M2M system starts with understanding the potential threats. Threat modelling involves thinking about the system or asset that needs protection and identifying how it can be compromised, either by remote attack or by a malicious insider. Threat modelling therefore begins in the software architecture stage and continues through the design phase.

When designing the system, threat should be analysed from the perspective or point of view of an attacker. Threat modelling, also called Architectural Risk Analysis, is a security control to identify and reduce risk. An example of Threat Modelling is the STRIDE Threat Model, (see Figure 4) STRIDE is a threat classification model developed by Microsoft), which helps place threats into categories such as Repudiation, Information disclosure, tampering with data, Denial of service, spoofing identity etc, and it includes a full breakdown of processes, data storage, data flows and trust boundaries.

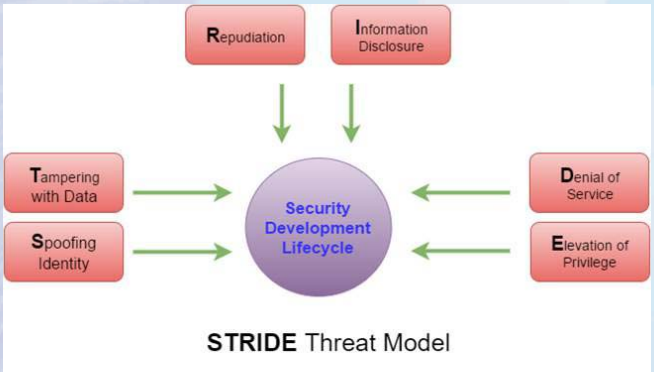


Figure 4

Securing an M2M system starts with understanding the potential threats. Threat modelling involves thinking about the system or asset that needs protection and identifying how it can be compromised, either by remote attack or by a malicious insider. When conducting this activity, it is important to remember that threats are not vulnerabilities. Vulnerabilities can be fixed; threats exist in perpetuity and are the attacker's goal.

[Prepared by Smart Network Division, TEC]

Mandatory Testing and Certification of Telecom Equipments (MTCTE)

A zonal workshop with objective of spreading the awareness among various stakeholders of MTCTE were held at Kolkata and Guwahati on 4th October'18 and 12th Dec'18 respectively. Workshop for various stakeholders viz. representatives of OEM companies, importers, Telecom Service Providers and industry associations was held in forenoon session whereas afternoon session was dedicated for Test Laboratories, so that more focused and dedicated discussion can be held with the stakeholders. Both the workshops were widely participated by the stakeholders. Participants of the workshops were mainly from respective Zones and many of them were first time attendee of Zonal workshop meeting. Queries raised by the participants were clarified by DDG (TC) and DDG (MRA). Demo of the MTCTE portal was also made which was primarily aimed upon demonstration of newly added features and to address the queries related to portal. The outreach programme was much appreciated by the participants.

MTCTE Portal was also launched in Nov-2018 to administer the mandatory testing & certification of telecom equipment.

Zonal workshop on MTCTE held at Kolkata on 4th October, 2018

Acceptance of IoT use case document in ITU-T SG-20 meeting, China, Dec 2018

Continuous efforts and participation by IoT division of TEC in SG-20 meetings in the last 2-3 years have resulted the acceptance of the use case document in ITU-T SG-20 meeting held in China, Dec 2018. This document is being published by ITU and will be available on SG-20 webpage. This meeting was attended by officers of IoT division remotely. Following use cases were standardized based on Indian contribution.

i. Vehicle emergency call system for automotive road safety

ii. Digitization and automation of Vehicle Tracking, Safety, Conformance, Registration and Transfer via the application of e-SIM and Digital Identity

iii. Remote monitoring the health of a patient

iv. Connected Smart homes.

v. Advanced Metering Infrastructure

These use cases may be implemented to create smart infrastructure, which will resolve number of issues of the respective vertical and in turn improve the quality of life.

Activities at NTIPRIT (OCT-18 to DEC-18)

1. Foundation Course for ITS-2014, P&T BWS-2013 and P&T BWS-2015 Batch Officer Trainees at HIPA Gurugram Haryana:

As part of Induction Training, 15 Officer Trainees of ITS-2014, 1 Officer Trainee of P&T BWS-2013 and 1 Officer Trainee of P&T BWS-2015 batch, joined 15 weeks Foundation Course at HIPA, Gurugram, Haryana. The Foundation Course was inaugurated on 17.12.2018 by Sh. Anil Kumar Sanghi, Sr. DDG,

Group Photograph of ITS-2014, P&T BWS-2013 and P&T BWS-2015 Batch Officer Trainees with faculties of NTIPRIT and HIPA on Inaugural Day of Foundation course at HIPA, Gurugram

Telecommunication Engineering Centre
Conference on M2M / IoT Enabling Smart Infrastructure
&
Release of Technical Reports on M2M/IoT
Shri Manoj ... na
SRT
AVC-31

Conference on M2M/IoT on 08.01.2019- Group Photo

NTIPRIT, Ghaziabad and Dr. G. Prasanna Kumar, Director General, HIPA, Gurugram. Sh. Rakesh Kumar Sharma, DDG (Admin.); Mrs. V Sobhana, DDG (Training); Sh. Subhash Chand, Director (Training); Sh. Manoranjan, ADG (Training) were also present during the inaugural event from NTIPRIT.

2. Joining of JTO-2016 (RL) batch for 30 Weeks Induction Training at NTIPRIT:

NTIPRIT has commenced Induction Training for a new batch of JTO Trainees on 03-12-2018. Besides Administrative and Establishment modules, they will get exposure on different telecom technologies.

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

3.1In-Service course on Role of Telecom in Disaster Management (09-10-2018 to 10-10-2018)

Two days In-Service course on Role of Telecom in Disaster Management was conducted at NTIPRIT. During the course the experts from government organizations were invited to deliver the lectures and share the experiences in the Disaster Management domain.

3.2In-Services Course on Trends in Telecom Licensing (04-12-2018 to 05-12-2018)

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

i. ITS-2015 batch (33 officers)
ii. ITS-2016 batch (34 officers)
iii. BWS-2015 batch (1 officer)
iv. BWS-2016 batch (3 officers)
v. BWS-2017 batch (2 Officers)
vi. JTO-2016(RL) Batch (2 officers)

हिंदी कार्यशाला का आयोजन

दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली में दिनांक 06.12.2018 को एक हिंदी कार्यशाला का आयोजन किया गया। इस कार्यशाला में कुल 24 अधिकारियों/ कर्मचारियों ने भाग लिया । इस कार्यशाला में अतिथि वक्ता के रूप में श्री पी सी विश्वकर्मा, परामर्शदाता राजभाषा, दूरसंचार विभाग ने भाग लिया। उन्होंने राजभाषा अधिनियम 1963 की धारा 3(3), राजभाषा नियम 1976, संसदीय राजभाषा समिति, नगर राजभाषा कार्यान्वयन समिति, हिंदी सलाहकार समिति, केंद्रीय हिंदी समिति आदि के बारे में विस्तार से उल्लेख किया। श्री विश्वकर्मा जी ने पत्राचार ज्यादा से ज्यादा हिंदी में करने तथा अंग्रेजी में प्राप्त पत्रों के उत्तर भी हिंदी में देने को कहा। उन्होंने हिंदी के बारे में काफी ज्ञानवर्धक जानकारी उपलब्ध कराई।

हिन्दी कार्यशाला में उपस्थित अधिकारी – कर्मचारी गण

Approvals from OCT-18 to DEC-18

Sl. No.	Name of the Manufacturer/Trader & Name of Product & Model No.
A	Nx Value Solutions India Pvt. Ltd.
1	PABX For Network Connectivity, Sonus SBC 2000
B	Sunren Technical Solutions Pvt. Ltd.
2	Electronic PABX, Sonus SBC 1000
C	ECI Telecom India Pvt. Ltd.
3	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 1G, NPT1200
4	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 10G, NPT1200
5	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 1G, NPT1050
6	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 10G, NPT1050
D	Ericsson India Pvt. Ltd.
7	Integrated Media Gateway, IP Media Gateway M-MGW-I
E	ALE India Pvt. Ltd.
8	PABX For Network Connectivity, OmniPCX office
F	Tejas Networks Ltd.
9	Interchange of STM-1, STM-4, STM-16 and STM-64 signals between different networks, STM-16 TM/ADM TJ1400
10	Interchange of digital signals at 2 Mbit/s, 8 Mbit/s, 34 Mbit/s, 45 Mbit/s and 140 Mbit/s ports, PTN Product TJ1400P-D
11	Interchange of STM-1, STM-4, STM-16 and STM-64 signals between different networks, STM-64 TM/ADM TJ1400
12	Interchange of digital signals at 2 Mbit/s, 8 Mbit/s, 34 Mbit/s, 45 Mbit/s and 140 Mbit/s ports, STM-64 TM/ADM TJ1400

Important Activities of TEC during OCT 18 to DEC 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/SDs/ERs issued:

- GR on 10G capable symmetric passive optical network (XGS-PON) technology for FTTX based broadband applications
- GR on FTTX based broadband access applications using Gigabit Passive Optical Network(GPON) Technology with Mini-OLT
- GR on 10G passive optical network (XG-PON) technology for FTTX based broadband applications
- IR on Trunk Media Gateway
- Amendment of GR on Adhesive PVC tape

DCC meeting conducted for:

- SR on IDMS using CAP
- SD on Calibration of EMF Measuring Instrument
- GR on 100G Ethernet traffic analyser(HH)
- GR on Radio Frequency Monitoring System

Sub DCC meeting conducted for:

- GR on NTP, GR on PRC
- GR on Multi-function portable device for e-KYC and Bill Payment having Bio-metric scanner, portable thermal printer
- IR on ISDN CPE, IR on ISDN NT1
- SD on Data dictionary, SR on Time Synchronization

Representation of TEC in various Training/ Seminar/ Meetings

- ITU-T SG-15 meetings at Geneva
- Remotely attended ITU-T SG20 & SG-12 meeting in Dec 2018
- E-meeting of ITU-T SG-20 in OCT2018
- BIS meeting organised by BIS in New Delhi
- Workshop on '5G' organised by TSDSI & IEEE in New Delhi
- 15th International conference on EMI/EMC 'INCEMIC 2018' in Bangalore
- Workshop on Advance Spectrum organised by GSMA at New Delhi
- Workshop on Public Procurement of Telecom Products and services in New Delhi
- Conference on EMI/EMC by M/s R & S in New Delhi
- SES workshop on Satellite Communication in New Delhi
- TAG Subcommittee meeting on In flight Connectivity held in TEC

Study/white paper issued:

- Security aspects of blockchain

Contributions submitted to ITU-T/R/D

- 03 contributions in SG-13 & SG-15 and 02 contribution in SG-12 were submitted in ITU-T

Other Activities

- Meetings of NWG – 11, 12, 13 & 17 in TEC
- 05 new Labs have been designated as CAB between oct-18 to Dec-18 and now total 31 Labs have been designated
- Various Technical presentations were given by stakeholders in TEC (i.e. Timing Requirements in Telecom Network by M/s Microsemi, NFVI & SD-WAN solutions by M/s Vmvare, IoT Security by M/s Trusted Objects, Embedded SIM and IoT data security by Taisys)
- A workshop on Artificial Intelligence, Blockchain and 5G process was organised with IEEE in TEC.
- Webinar on 'Security aspects of Blockchain' and 'Role of IT in disaster management' conducted in TEC.
- One-day training programme on OneM2M was organised by M/s Interdigital in TEC

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
जनवरी 2019 : खुर्शीद लाल भवन
भाग 23 : जनपथ
अंक 1 : 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