Azadi Ka Amrit Mahotsav

ISO 9001:2015

Event: ETSI Security week, 16-19 Oct 2023

Session: IoT Security – Initiatives taken in TEC, DoT, India

Oct 16, 2023

Sushil Kumar
Deputy Director General
Telecommunication Engineering Center
Department of Telecommunications
Government of India

Telecommunication Engineering Centre (TEC)

ISO 9001:2015

- National Standards Body (NSB) for Telecom & related ICT sector
- Designated National Enquiry point for WTO –TBT (Technical Barrier to Trade) for telecom sector.
- Mandated to coordinate with ITU-T and having National Working Groups (NWGs) in line with ITU-T Study Groups (11 study groups). DoT is the nodal agency for coordinating with ITU from India.
- Also participating in ETSI, oneM2M, 3GPP standardisation activities at global level; and in TSDSI and BIS in India.
- Designated authority to implement Mandatory Testing & Certification of Telecom Equipment (MTCTE)
- Designated authority to accredit the CABs (Conformity assessment bodies)

- **Related to IoT and Smart City Standardisation activities**

  Participating in the meetings of ITU-T SG-20, ITU-T SG-17, ITU-R WP 5D, ITU-T FG AI4A, ISO/ IEC JTC1 SC41, ETSI IoT week / Security weeks, oneM2M, 3GPP, NIST etc. at international level; and in Bureau of Indian Standards (BIS) & Telecom Standards Development Society of India (TSDSI) at National level.

Policy initiatives for of M2M/ IoT & 5G in India

1. Important policy points released by Department of Telecom (DoT)

- **National Digital Communication Policy (NDCP)-2018** released in 2018 having salient features:
  - **Secure & Sustainable** eco-system development for massive scale of **5 billion connected devices,**
  - Simplifying licensing and regulatory framework whilst ensuring appropriate ***security framework for IoT/ M2M/ future services and network elements incorporating international best practices.***
  - ***Developing framework for accelerated deployment of M2M services while safeguarding security and interception for M2M devices.***
  - Creating a roadmap for emerging technologies and its use in the communications sector, such as **5G, Artificial Intelligence, Robotics, Internet of Things, Cloud Computing and M2M**
  - Establish a multi-stakeholder led collaborative mechanism for coordinating transition to **Industry 4.0**
  - Developing market for IoT/ M2M connectivity services in sectors including **Agriculture, Smart Cities, Intelligent Transport Networks, Multimodal Logistics, Smart Electricity Meter, Consumer Durables** etc. incorporating international best practices

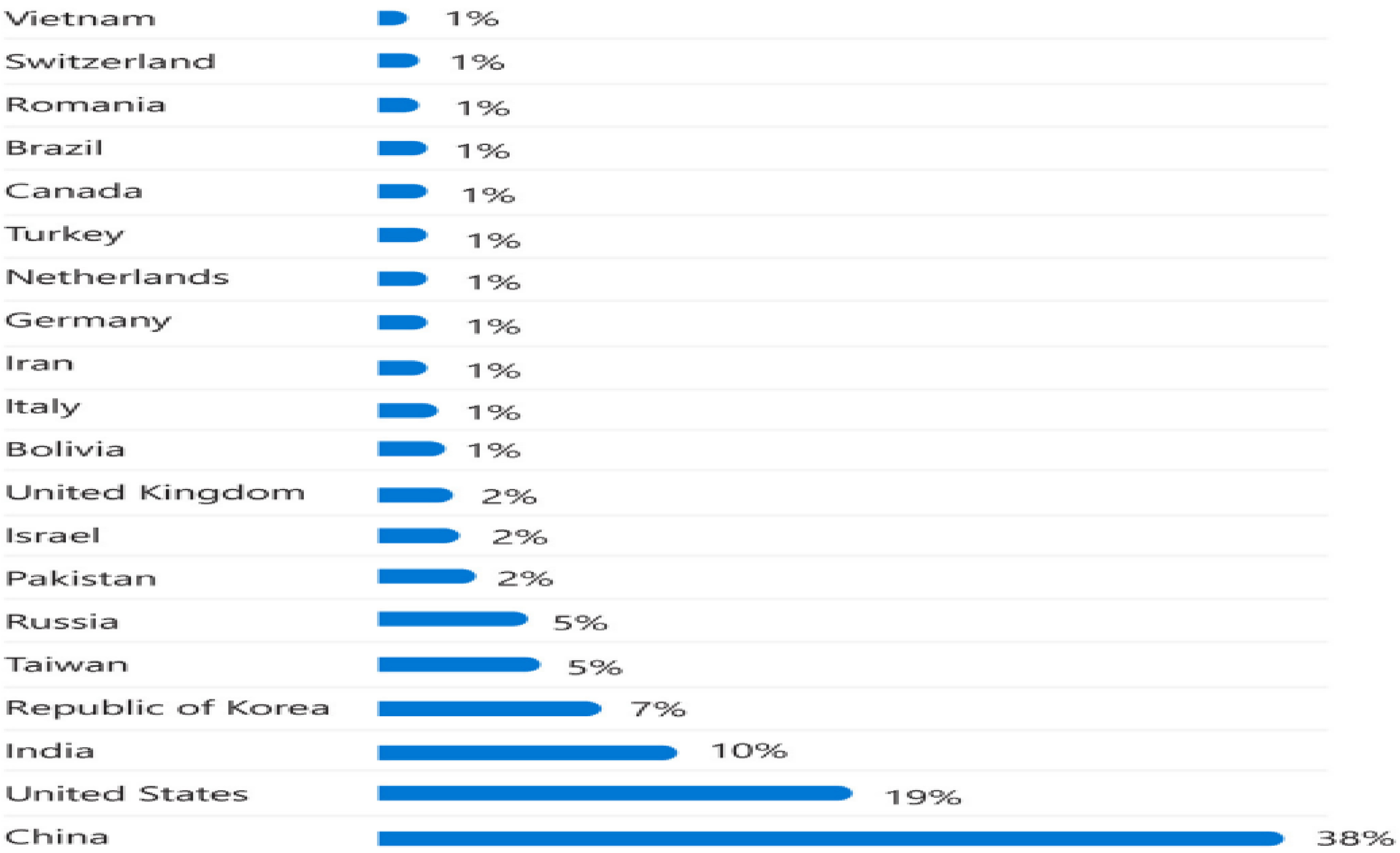
Policy initiatives for of M2M/ IoT & 5G in India

- Promoting research & development in Digital Communication Technologies by creating a framework for testing and certification of new products and services

- National Telecom M2M Roadmap released in 2015.
- M2M Service provider registration policy released in Feb 2022: M2M/ IoT Service providers should register on DoT portal.
- Production Linked Incentive (PLI) scheme for Promoting Telecom & Networking Products Manufacturing in India
- Telecom Technology development fund (TTDF) launched for indigenous development of technologies.
- Bharat 6G Alliance launched recently.

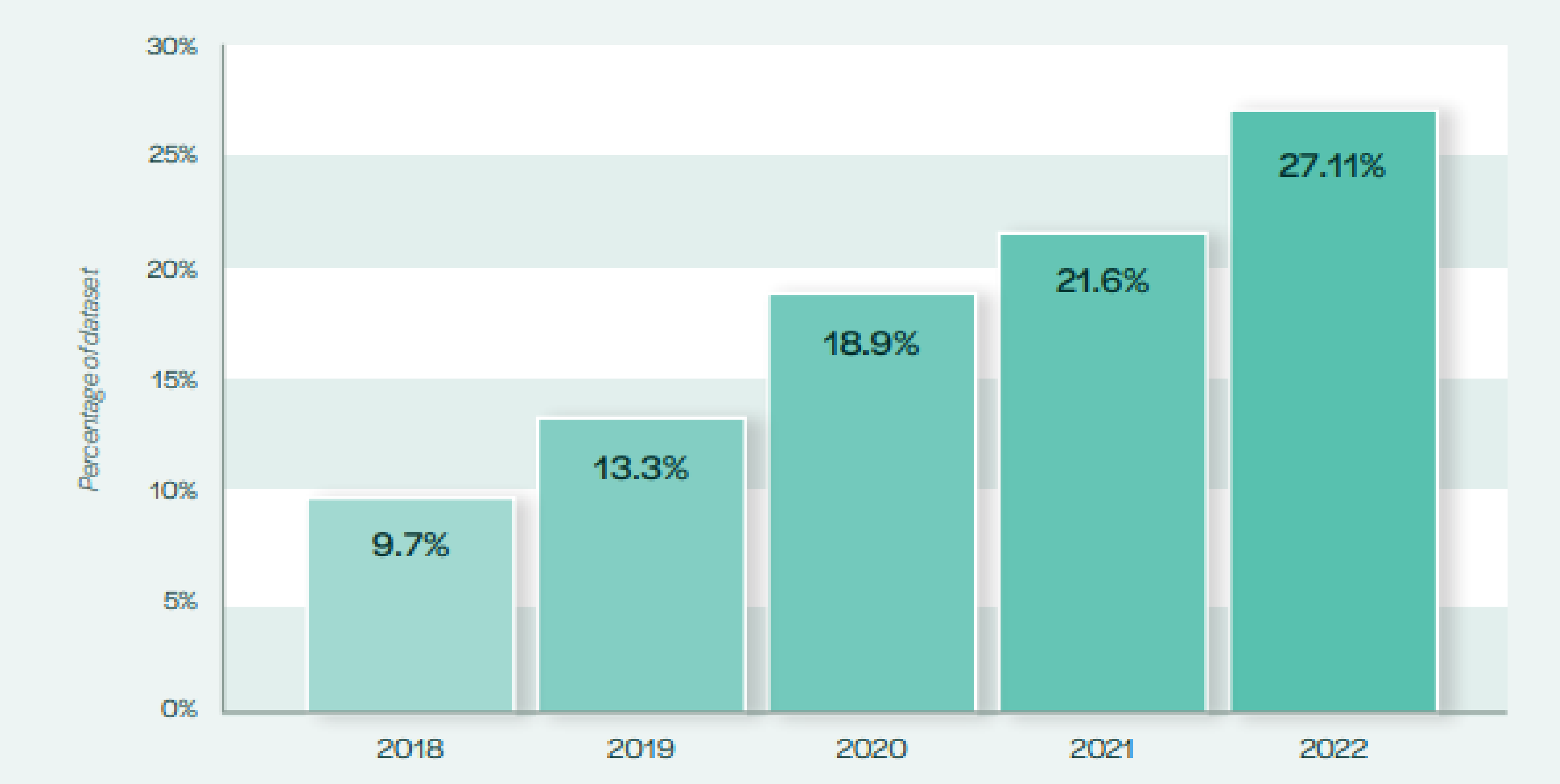
2. Ministry of Electronics & information technology (MeitY) released the policies on semiconductor development, electronics manufacturing etc.

Top countries originating IoT malware infection during 2022



Source: Cyber signals, Dec 2022

Vulnerability Disclosure statistics



Source: IoTSF

TEC Technical reports on M2M/ IoT security

- IoT Division, TEC released twenty one technical reports in M2M/ IoT domain covering various verticals, communication technologies, EMF radiation from IoT devices and IoT Security with the outcome intended to be used in policies/ standards (https://tec.gov.in/M2M-IoT-technical-reports).

- Three Technical Reports are related to IoT Security, released in the recent past:

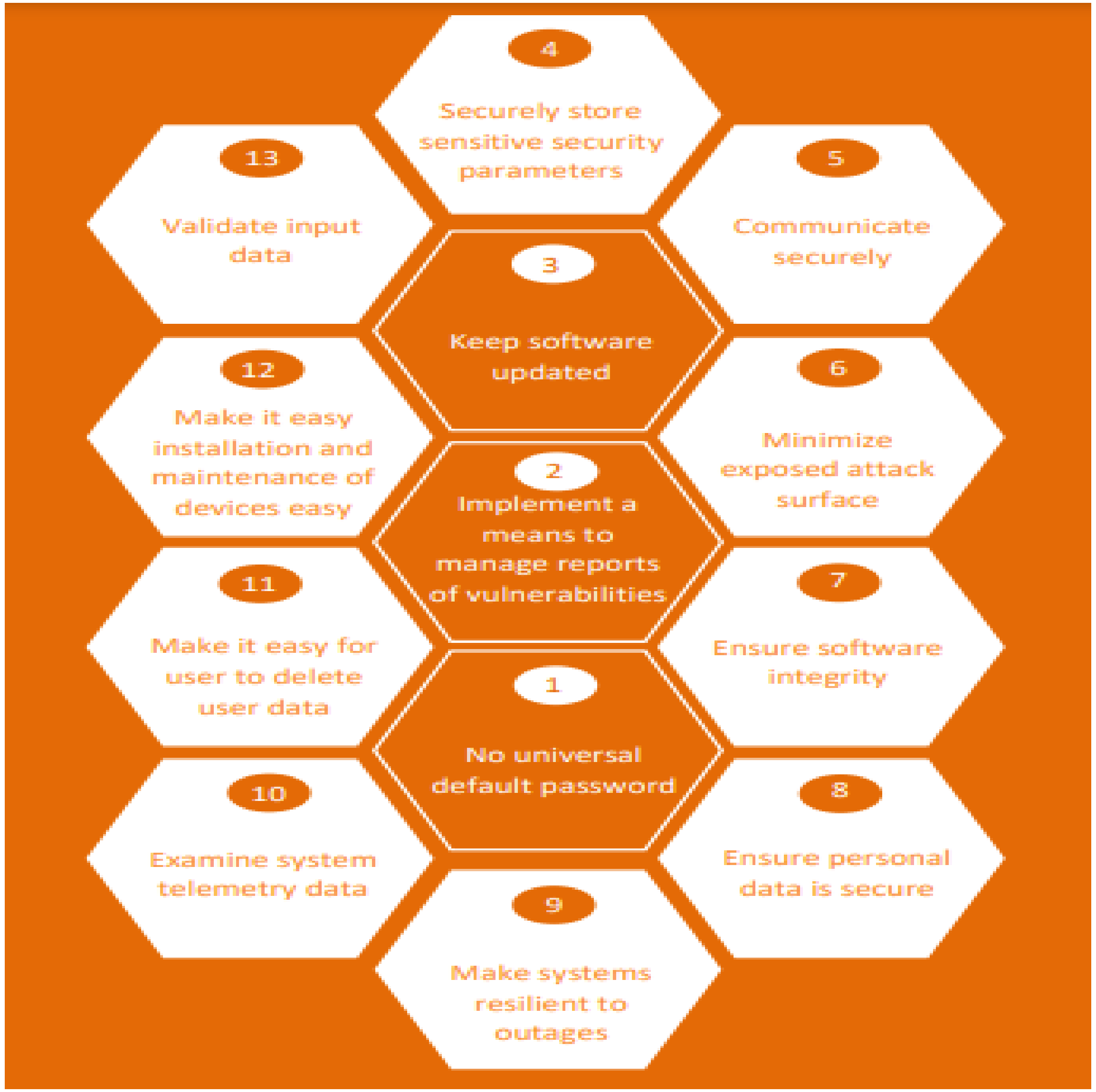
  1. *Security by design for IoT device manufacturers*, released in March 2023
  2. *Framework of National Trust Centre for M2M/IoT Devices and Applications*, released in March 2022
  3. *Code of Practice for Securing Consumer Internet of Things (IoT),* released in August 2021

- Envisaging the importance of these technical reports, ITU has posted Six TEC Technical reports including the above three on its global resource portal in IoT section (2023 – 2021) for the benefit of global community (https://www.itu.int/cities/dt-resource-hub/iot/) .

- Code of practice for Securing Consumer IoT has been mentioned by several international organizations such as in

  1. *Contemporary use of Vulnerability disclosure in IoT* released by IoTSF in Nov 2021.
  2. *Consumer IoT Device Cybersecurity Standards, policies and certification schemes*, released by OMDIA in Feb 2022.

1. Code of Practice for Securing Consumer IoT, released by TEC in Aug 2021, based on ETSI TS 103 645 principles:



1 No universal default password

2 Implement a means to manage reports of vulnerabilities

3 Keep software updated

4 Securely store sensitive security parameters

5 Communicate securely

6 Minimize exposed attack surface

7 Ensure software integrity

8 Ensure personal data is secure

9 Make systems resilient to outages

10 Examine system telemetry data

11 Make it easy for user to delete user data

12 Make it easy installation and maintenance of devices easy

13 Validate input data

- WEF Joint statement on consumer IoT Security released in Feb 2022, having the following guidelines as recommendations:

  a. No universal default passwords
  b. Implementing a vulnerabilities disclosure policy
  c. Keeping software updated
  d. Securely communicating
  e. Ensure that personal data is secure

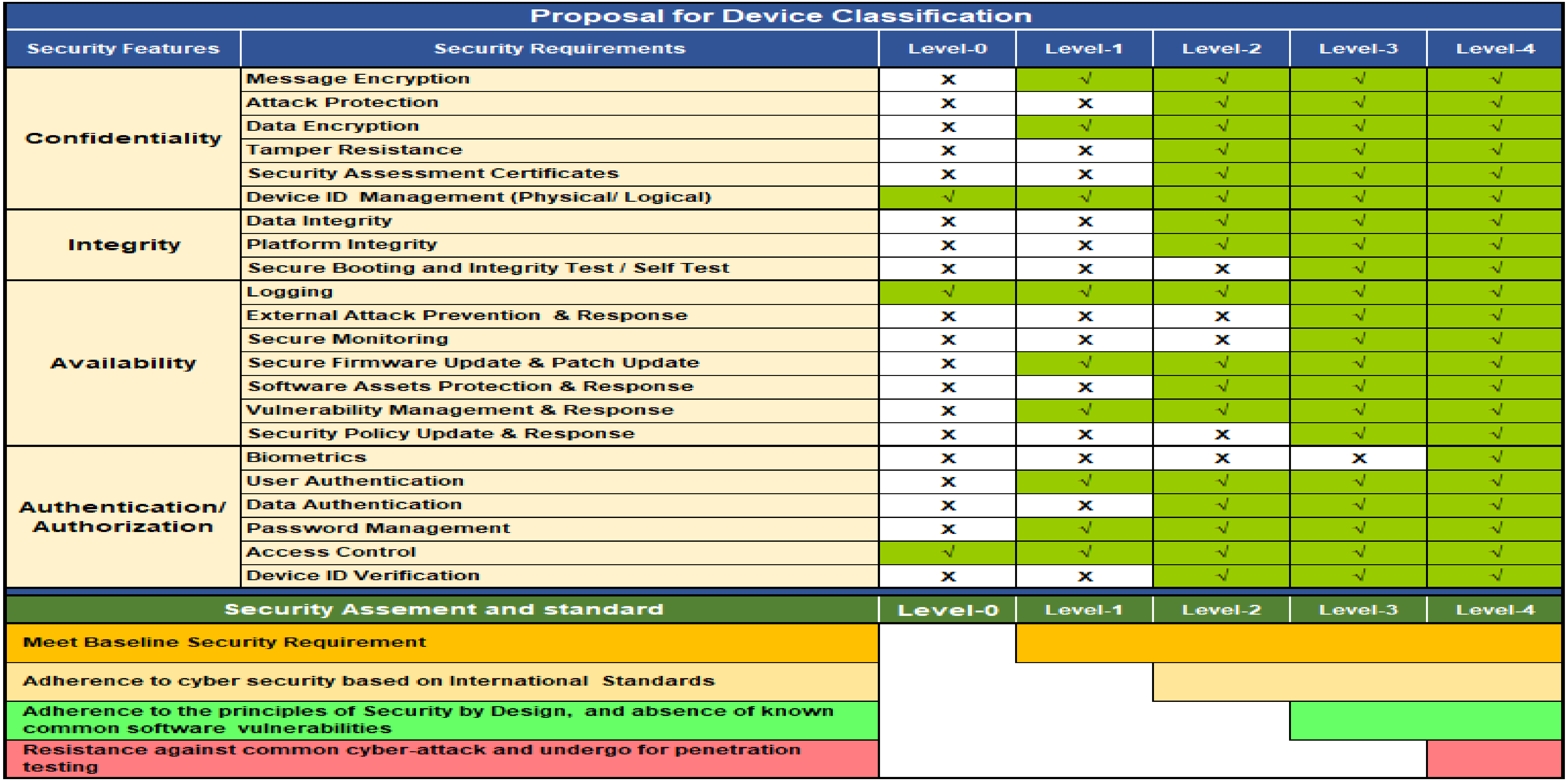
TEC Technical Reports on M2M/ IoT Secrity

2. The technical report on ***Framework of National Trust Centre (NTC) for M2M/ IoT Devices and Applications*** released in March 2022 visualizes the implementation of national trust centre in a phased manner for managing/ addressing the vulnerability related issues of the IoT devices reported by IoT/ Smart city platforms working in the network. NTC project is being developed by Center for development of telematics (C-DOT).

3. Technical Report ***Security by design for IoT Device Manufacturers*** released in March 2023, highlights various threats and challenges related to IoT device security; includes study of national/ international standards (by **ITU, ISO/ IEC, ETSI, ENISA, IoTSF, NIST, GSMA, 3GPP** etc.), best practices and guidelines (**UK DCMS, CSA Singapore, WEF, STQC** etc.) to mitigate these challenges. This report also provides recommendations for IoT device manufacturers and related stakeholders including policy makers, which will help in securing IoT ecosystem.

Recommendations are being included in the security requirements being developed for testing & certification of the products.

Proposed IoT devices classification for India



Proposal for Device Classification

Security Features	Security Requirements	Level-0	Level-1	Level-2	Level-3	Level-4
Confidentiality	Message Encryption	x	√	√	√	√
	Attack Protection	x	x	√	√	√
	Data Encryption	x	√	√	√	√
	Tamper Resistance	x	x	√	√	√
	Security Assessment Certificates	x	x	√	√	√
	Device ID Management (Physical/ Logical)	√	√	√	√	√
Integrity	Data Integrity	x	x	√	√	√
	Platform Integrity	x	x	√	√	√
	Secure Booting and Integrity Test / Self Test	x	x	x	√	√
Availability	Logging	√	√	√	√	√
	External Attack Prevention & Response	x	x	x	√	√
	Secure Monitoring	x	x	x	√	√
	Secure Firmware Update & Patch Update	x	√	√	√	√
	Software Assets Protection & Response	x	x	√	√	√
	Vulnerability Management & Response	x	√	√	√	√
	Security Policy Update & Response	x	x	x	√	√
Authentication/ Authorization	Biometrics	x	x	x	x	√
	User Authentication	x	√	√	√	√
	Data Authentication	x	x	√	√	√
	Password Management	x	√	√	√	√
	Access Control	√	√	√	√	√
	Device ID Verification	x	x	√	√	√

Security Assement and standard	Level-0	Level-1	Level-2	Level-3	Level-4
Meet Baseline Security Requirement		▨	▨	▨	▨
Adherence to cyber security based on International Standards			▨	▨	▨
Adherence to the principles of Security by Design, and absence of known common software vulnerabilities				▨	▨
Resistance against common cyber-attack and undergo for penetration testing					▨

Initiatives taken by TEC, DoT India on IoT Security

1. Department of Telecom, policy maker in India, has endorsed TEC Technical Report ***Code of practice for securing consumer IoT*** to all the related stakeholders including M2M Service providers to follow *at least the f*irst three guidelines as listed below:

   (a). No universal default passwords i.e. Ban default password.

   (b). Implement a means to manage reports of vulnerabilities. (c). Keep software updated

These guidelines are expected to be mandated in near future, making them as a minimum base line requirements.

2. M2M Service providers have to register with DoT and follow the registration guidelines.

3. Indian Telecom Security Assurance Requirements (ITSAR) for IoT devices will be based on IoT devices classification proposed for India.

Initiatives taken by TEC, DoT India on IoT Security

Recommendations available in **Security by design for IoT device manufacturers** are being considered to be the part of ITSAR/ other policy guidelines for the stake holders. These are H/W Security, S/W Security, Policy recommendation and Generic. Some of them are listed below:

1. Secure on boarding of IoT devices at the platform preferably using ITU-T X.509 standard for digital certificates.

2. Life expired devices or the devices not getting updates may be highly vulnerable and threat to the network. Suitable policy mechanism is required to replace such type of devices.

3. Platform / NTC is expected to analyse

    i. Average response time / patch release time for critical vulnerabilities by product
    ii. Percent/ number of products no longer receiving security updates in operation.

4. Consumer awareness regarding Vulnerabilities / security of IoT products.

5. Every consumer device should have a forced mechanism for changing the password by the user prior to its first use.

Initiatives taken by TEC, DoT India on IoT Security

6. Platform providers are also the M2M/ IoT Service providers. All the M2M/ IoT Service providers should register with DoT. Other entities like M2M/ IoT device manufacturers, application providers, network providers etc. should also register on DoT portal.

7. TSPs should provide the telecom resources only to the registered M2M/ IoT Service providers with DoT.

8. IoT device manufacturer should test the devices against known vulnerabilities before release. To begin with critical devices and network elements such as IoT Gateway, Smart Camera, Wi-Fi routers, ONT etc. may be taken.

9. Related Standard Operating Procedure (SoP) and ITSARs should be implemented and regular audit mechanism should be in place.

10. For promoting IoT security, domestic IoT device Manufacturers and other stakeholders, as applicable, may be incentivized for a limited period for adopting the IoT security baseline requirements.

11. IT infrastructure of OEM initiating the Software update (Patch loading) should be registered and operated from Indian Territory.

Initiatives taken by TEC, DoT India on IoT Security

12. IT infrastructure of OEM initiating the Software update (Patch loading) should be registered and operated from Indian Territory.

13. IT infrastructure related to eSIM remote service provisioning (SM-DP, SM-SR and SM-DP+) need to be owned by any registered entity with DoT and located within Indian territory.

14. NTC should be developed on priority as it will help in managing vulnerabilities/ security related issues.

THANKS

For detail, see the TR available on www.tec.gov.in/technical-reports/

Sushil Kumar
Dy. Director General (IoT)
Telecommunication Engineering Center(TEC)
+919868131551
Sushil.kumar20@gov.in
sushil.k.123@gmail.com
in.linkedin.com/in/sushil-kumar-98895560