Draft Guidelines / Code of Practice

for

Securing

Consumer Internet of Things (IoT)

Table of Contents

Executive summary

IoT is one of the most emerging technology across the globe and is being used to create smart infrastructure in various verticals using connected devices. IoT is benefitted by recent advances in several technologies such as Sensor, communication technologies (Cellular and non cellular), AI/ ML, Cloud computing, Edge computing and mobile edge computing.

As per the Ericsson mobility report, June 2020, there may be 24.6 Billion connected devices globally by 2025. Out of this around 21% will be on cellular technologies.

As per the study by GSMA, there may be around 11.4 Billion consumer IoT devices and 13.3 Billion enterprise IoT devices by 2025.[1]

As per the NDCP released by DoT, eco-system is to be created for 5 Billion connected devices by 2022, therefore around 60% i.e. 3 Billion connected devices may exist in India by 2022. Out of this there may be 50:50 consumer : Enterprise connected devices.

To maintain security of the network, only the certified devices should be allowed to connect in the network. Additionally, new vulnerabilities may be discovered in the already certified devices. Therefore, a central mechanism like National Trust Center (NTC) is required to ensure the deployment of the certified devices and addressing the vulnerabilities.

TRAI released recommendations on on Spectrum, Roaming and QoS related requirements in Machine-to-Machine Communications' in September 2017. These recommendations were accepted by DoT. Two recommendations as mentioned below were sent to TEC to carry forward the work.

1. Device manufacturers should be mandated to implement "Security by design" principle in M2M devices manufacturing so that end to end encryption can be achieved.

2. A National Trust Center (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software). *This recommendation was accepted in principle by DoT.*

TEC has been working on Security by design principles and National trust center on IoT in a multi-state holders WG. Study is in progress taking into account the standards and best practices being used across the globe. These guidelines are the part of the documents under discussion and a step in the direction of implementing the National Trust center.

[1] https://enterpriseiotinsights.com/20200305/5g/iot-connections-reach-almost-25-billion-globally-2025-gsma

Introduction

IoT / M2M technology is being used to create smart infrastructure in various verticals such as Power, Automotive, Safety, Surveillance, Health care, Agriculture, Smart homes and Smart cities etc. Security of the IoT domain i.e. from devices to the applications is very important as the hacking of the devices / networks being used in daily life will harm to companies, organisations, nations and more importantly people. It may result in collapse of the services, creating panic and havoc. Ensuring end to end security for connected IoT devices is key to the success in this market - without security, IoT will cease to exist. Apart from security, privacy of the data of the individuals is another very important domain especially in the health care sector. According to a new market research report published by Markets and Markets, the global Internet of Things (IoT) Security Market size is expected to grow from USD 8.2 billion in 2018 to USD 35.2 billion by 2023, at CAGR of 33.7 percent during the forecast period[2].

IoT devices, services and software, and the communication channels that connect them, are at risk of attack by a variety of malicious parties, from novice hackers to professional criminals or even state actors. Possible consequences of such an attack could include:

- Inconvenience and irritation
    - Discontinuity and interruption to critical services/infrastructure
- Infringement of privacy
- Loss of life, money, time, property, health, relationships, etc.
- Disruptions of national scale including civil unrest.

For vendors, operators and suppliers, potential consequences may include loss of trust, damage to reputation, compromised intellectual property, financial loss and possible prosecution.
Malicious intent commonly takes advantage of poor design, but even unintentional leakage of data due to ineffective security controls can also have dire consequences to consumers and vendors. Thus it is vital that IoT devices and services have security designed in from the very outset.

IoT Security Foundation released a report on vulnerability disclosure based on a survey of 330 IoT manufacturers in 2018 and 2019. In 2018 only 9.7% (32) manufacturers were reporting vulnerability, which increased marginally in numbers as to be 13.3% (44) in 2019. Companies under survey were from North America, Asia and Europe.

[2] https://www.marketsandmarkets.com/PressReleases/iot-security.asp

This is of great concern as vulnerability disclosure is widely considered to be a baseline requirement due to its fundamental importance towards operational IoT security.

This report has mentioned that only few companies are working on vulnerability disclosure despite Incoming Laws and International Standards.
It is imperative that the providers of IoT products need to implement the vulnerability disclosure policy on priority.

Available standards in Consumer IoT domain:- ETSI has released ETSI EN 103645 (V 2.1.2) in June 2020 on **Cyber Security for Consumer Internet of Things: Baseline Requirements.** It is having 13 basic principles.

ETSI 103645 has been adopted by EU as ETSI EN 303 645. ETSI TC CYBER is taking forward TS 103 701, which will set out test scenarios for assessing products against EN 303 645.

Code of practice released by UK in 2018 and Australia in 2020 are also based on 13 principles mentioned in ETSI 103 645.

USA has come with the policy and asked NIST to prepare the standards for it. Singapore has released Cyber security labelling scheme.

This document is being created for the following stakeholders :

- **IoT Device Manufacturers**
- **IoT Service Providers / System integrator**
- **Mobile Application / IoT Application Developers**
- **Component Providers**
- **Consumer**

Types of consumer IoT devices

This Code of Practice applies to consumer IoT products that are connected to the internet and/or home network and associated services. A non-exhaustive list of examples are as given below:

- Connected wearable healthcare devices,
- Smart cameras, TVs and speakers,
- Connected children's toys and baby monitors,
- Connected safety-relevant products such as smoke detectors, and door locks,
- Connected home automation and alarm systems,
- Connected appliances (e.g. washing machines, fridges),
- Smart home assistants.
- IoT gateway like WiFi router, Smart phones

The security assurance level required by these applications vary across applications and services.

'Associated services' are here considered as the digital services that are linked to IoT devices, for example mobile applications, cloud computing/ storage and third party Application Programming Interfaces (APIs) to services such as messaging.

Guidelines

1. No universal default passwords

All IoT device default passwords shall be unique and not resettable to any universal default value.

Many IoT devices are being sold with universal default usernames and passwords (such as 'admin, admin') which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed. Associated web services should use Multi-Factor Authentication, not provide any unnecessary user information prior to authentication, and any password reset process should appropriately authenticate the user[3].

Primarily applies to: IoT Device Manufacturers

2. Implement a means to manage reports of vulnerabilities

IoT device manufacturers, IoT service providers / System integrators and Mobile application developers should provide a public point of contact as part of a vulnerability disclosure policy in order for security researchers and others to report issues. Disclosed vulnerabilities should be acted on in a timely manner. Implementing a bug bounty program encourages and rewards the cyber security community for identifying and reporting vulnerabilities, thereby facilitating the responsible and coordinated disclosure and remediation of vulnerabilities.

Primarily applies to: IoT Device Manufacturers. IoT service provide / System integrator and Mobile Application developer.

3. Keep software updated

Developing and deploying security updates in a timely manner is one of the most important actions a manufacturer can take to protect its customers and the wider technical ecosystem. It is good practice that all software is kept updated and well maintained.

Software components in IoT devices should be securely updateable. Updates shall be timely and should not impact the functioning of the device. An end-of-life policy shall be published for end-point devices

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
NIST, 2017, 'NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management', https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement, preferably using non-intrusive approaches like over the air (OTA) updates . For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

Software updates should be provided after the sale of a device and pushed to devices for the lifecycle of the device. This period of software update support shall be made clear to a consumer when purchasing the product. The retailer and/or manufacturers should inform the consumer that an update is required. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear. An important feature associated to this practice is protection against rollback, to prevent a software update to a version of software that is illegal or unsafe.

If a user interface is available it should clearly display when a device has reached its end-of-life, inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk.

Primarily applies to: IoT Device Manufacturers. IoT service provide / System integrator and Mobile Application developer.

4. Securely store sensitive security parameters

Any credentials should be stored securely within devices and on services. Hard-coded credentials (e.g. Userid, passwords, access keys) should not be embedded in device software or hardware since they can be discovered via reverse engineering.

. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys, device identifiers and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment (TEE) and associated trusted, secure storage.

Depending on the requirements, a trusted storage may be enough (i.e. in protection of data for confidentiality and integrity by TEE) but in other cases a secure storage may be needed (i.e. in protection of storage against physical tampering). Such a means ensure that HW level protection is available for critical building blocks of the device with the ability to encrypt and protect/allocate critical sections of the memory for secure processing, ability to detect, validate and process SW updates securely in the field.

Primarily applies to: IoT Device Manufacturers. IoT service provide / System integrator and Mobile Application developer.

5. Ensure Communicate securely

Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely. Depending on the requirement, a TEE may be enough. If needed this can be coupled with a secure element (SE) that stores the credentials.

When configuring a secure connection, if an encryption protocol offers a negotiable selection of algorithms, remove weaker options so they cannot be selected for use in a downgrade attack.

All remote access should be logged, with logs including the date, time and source of access at a minimum.

All unrequired ports (physical and network), interfaces should be disabled. Authenticate peer before sending any data or acting on received data.

Primarily applies to: IoT Device Manufacturers. IoT service provide / System integrator and Mobile Application developer.

6. Minimize exposed attack surfaces

Devices and services should operate on the 'principle of least privilege'. Unused functionality should be disabled; hardware should not unnecessarily expose access (e.g. unrequired ports should be closed, the web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet); functionality should not be available if they are not used; and code should be minimised to the functionality necessary for devices and services to operate. Software should run with appropriate privileges, taking account of both security and functionality. To further reduce the number of vulnerabilities, use a secure software development process and perform penetration testing.

The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

Primarily applies to: IoT Device Manufacturers. IoT service provide / System integrator

7. Ensure software integrity

Software (including firmware) on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

During the boot sequence, wherever possible, check that only the expected hardware and peripherals are present and matches the current configuration parameters. Boot should fail graceful, if it fails should never reveal an elevated permissions interface.

Consequently, software authenticity is also important (i.e., avoid the usage of software provided by an unauthorized source). In addition, it is necessary to ensure that the software is loaded only on an authorized device (i.e. to avoid a legal software to run on an illegal device)

Primarily applies to: IoT Device manufacturer

8. Ensure that personal data is secure

Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the Data Personal Data Protection bill 2018. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this shall be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.

Several other principles in this document are related to protecting personal data, such as installing and securely configuring

This guideline ensures that:

i. IoT manufacturers, service providers and application developers adhere to data protection obligations when developing and delivering products and services;

ii. Personal data is processed in accordance with data protection law;

iii. Users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified;

iv. Users are provided with means to preserve their privacy by configuring device and service functionality appropriately.
v. Ensuring that the data remains 'fresh', i.e. preventing a rollback to old data.

Primarily applies to: IoT Device Manufacturers. IoT service providers / System integrator, Mobile Application developer and Retailers.

9. Make systems resilient to outages

Resilience should be built into IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT devices should remain operating and locally functional in the case of a loss of network, without compromising security or safety. They should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than all attempt to reconnect at the same time. Implementing redundancy and DDoS mitigation helps ensure that IoT services remain online. Architect IoT devices to continue functioning as much as possible if an associated IoT service becomes unavailable, and disclose upfront to the consumer which features will cease working in this case. IoT service providers should also update data when network connection is restored.

Means should exist to verify that the device was not altered / tampered during the period of connectivity disruption.

Primarily applies to: IoT Device Manufacturers. IoT service providers / System integrators

10.Examine system telemetry data

If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.

Constant monitoring of the device is necessary to handle operational and security issue in time. Ensure all logged data comply with prevailing data protection regulations. All logs and telemetry data should stored securely before it's sent to monitoring service, while communicating with the telemetry service, service should be authenticated and data should be encrypted. Access to telemetry data should be on need to know basis.

Primarily applies to: IoT Device Manufacturers. IoT service providers / System integrators

11.Make it easy for users to delete user data

Devices and services should be configured such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data, including how to reset the device to "factory default" and delete data stored on the device and in associated backend/cloud accounts and mobile applications.

A 'factory reset' function must fully remove all user data/credentials stored on a device.

Primarily applies to: IoT Device Manufacturers. IoT service providers / System integrator, Mobile Application developer

12.Make installation and maintenance of devices easy

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.

Primarily applies to: IoT Device Manufacturers. IoT service providers / System integrator, Mobile Application developer

13.Validate input data

The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

i. Not of the expected type, for example executable code rather than user inputted text.
ii. ii. Out of range, for example a temperature value which is beyond the limits of a sensor.

Primarily applies to: IoT Device Manufacturers. IoT service providers / System integrator, Mobile Application developer

Definitions

IoT Device Manufacturers

The entity that creates an assembled final internet-connected product. A final product may contain the products of many different manufacturers.

IoT Developers

Entities that develop and provide applications that run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.

IoT Service Providers

Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.

Consumer

Consumers may take many forms. Governments, businesses and individuals may all be consumers of IoT devices. This Code of Practice particularly focuses on consumer grade, internet-connected devices and associated applications (e.g. wearable devices, and home appliances such as “smart” televisions and refrigerators). This group of devices does not include mobile phones – as they are considered sophisticated devices and other guidance may more accurately apply.

Retailers

The sellers of internet-connected products and associated services to consumers.

Additional explanatory notes