सत्यमेव जयते

ITSAR Mobile Device

Indian Telecom Security Assurance Requirements

Mobile Device Security Requirements

Release Date: Version Number: 1.0.0

Effective Date:

National Centre for Communication Security
Department of Telecom, Ministry of Communications
Government of India

Table of Contents

1.0 Introduction

Mobile Device technology revolution has traversed a long distance within a short span from brick-like cellular phones with limited abilities to ultra-slim and powerful smartphones with abilities to do anything to everything. Smart Phones with their abilities to do complex of tasks at the ease of a simple touch, became ubiquitous in personal, social and professional life.

Along with their portability, mobility & ubiquitous presence, Emergence of M Commerce, M Health, M Banking and M Payments & Finance forced Mobile Devices to handle more sensitive data than Laptops/Computers ever handled. As Mobile applications collecting huge quantities of data and storing them on device/cloud, safety and privacy data in storage/transit needs to be addressed. Right to privacy being Fundamental Right and Data being new form of wealth, there need to be enough safeguards to protect the user’s privacy from ever evolving threats and unintended exploitation.

Emphasis on Digital Economy, Jandhan Aadhar Mobile (JAM) Trinity for delivering social welfare requires Mobile Device to play a pivotal role in realizing country’s larger goal of inclusive and sustainable development. Safe and secure devices play vital role in achieving the stated objective. As security of the system is as strong as its weakest link, it is essential to provide Minimum Security Baseline for the mobile devices across the ecosystem so that, sensitive data and identity of 1.2 Billion Indians are reasonably protected. This forms the basis for the need of this ITSAR.

1.1 Mobile Device Definition

For this document purpose Mobile Device covers all types of Mobile User Equipment like Mobile Handset i.e feature phone and smart phone, Tablets /Phablets or any other device having cellular interface and having other optional features as listed below,

(The following features are common, but optional, characteristics of mobile devices. These features do not define the scope of devices included in this document, but rather indicate features that are particularly important in terms of security risk. This list is not intended to be exhaustive, and is merely illustrative of common features of interest.)

- Advanced Operating System
- Typically hand held and Portable i,e Small form factor
- Designed to operate wirelessly. At least one wireless network interface for network access (data communication). This interface may use Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.

- Data storage capability
- Self-contained power source
- Applications, that can be installed from various sources (i.e. Provided with the mobile device (Built in), accessed through public/enterprise app store, accessed through web browser, acquired and installed from third parties)
- One or more digital cameras/video recording devices
- Microphone
- Built-in features for synchronizing local data with remote system (desktop or laptop computer, organization servers, telecommunications provider servers, other third-party servers, etc.)

Note1: Threat perceptions of Point of Sales Devices, Autonomous Vehicles, Desktops, Laptops, Robots ...etc are not considered and are out of scope for this document.

(Source: TEC ,Essential Requirements (TEC 47722002) for Mobile User Equipment

1.2 Mobile Device Usage

Though, Mobile is ubiquitous, considering the usage statistics, mobile device usage can be classified into 3 broad use case scenarios. They are,

- Mobile device for personal use.
- Mobile device for both enterprise and personal use (Mobile Device owned by enterprise)
- Mobile device for specialized, high security use

In this document we will be proposing security testing of all the Mobile Devices with varied rigours, i.e Level 1 Level 2 with progressive increase in rigour from Level 1 to Level 2. For more insights refer to Section 5.

1.3 Scope

Primary Objective of this document is to define ‘minimum security base line standard’ for Mobile Device Security, irrespective of the Make/Model/OS Platform of Mobile Device. The scope of this document also includes the following,

1. Mobile Device Technology Stack consisting of Hardware, Firmware, Operating Systems and Pre-Installed (Bundled) applications used for personal and enterprise use.
2. Identifying security threat perception of Mobile Device.
3. Identify and define Security Levels required for Mobile device security testing and its applicability to the Mobile Devices.
4. Defining Security Requirements for addressing Security Threats for Level 1 and Level 2 Security Testing

However, test schedules and test procedures, evaluation check points and evaluation methodology document will be released subsequently and outside the scope of the present document.

Targeted audience for the document: Mobile Device Designers, Mobile Device Manufacturers/OEMs, Testing Agencies, Quality and Assurance Groups, Security Engineers, Managers and Administrators, Telecom Service Providers and Others.

2.0 Mobile Device Technology Stack

In today’s market, mobile devices have complex architectures with hardware and software elements interoperating closely to offer rich user experiences without compromising on performance, safety, security and battery life. The architectural blueprint of most mobile devices includes the hardware modules, firmware code, the operating system and an application platform, as depicted in the diagram below

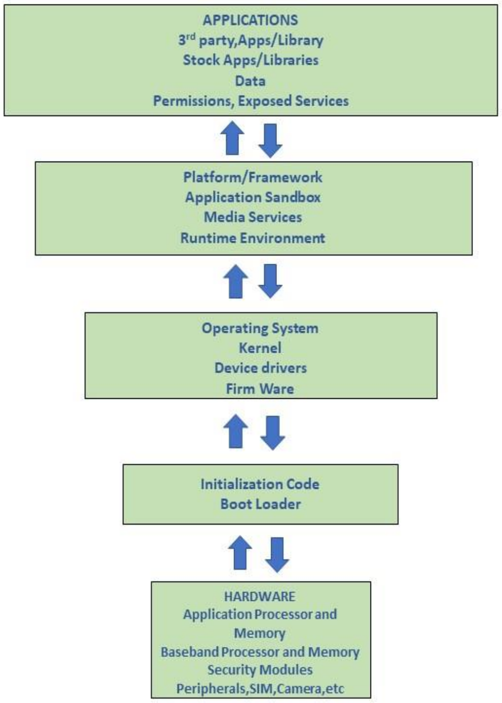

Fig 1. Illustrates the generic Mobile Device Technology stack and the components there on.

(Source Reference 9)

3.0 Mobile Device Ecosystem

Mobile devices operate in an ecosystem that includes not only the handset, but also a broad range of hardware and software stacks, various subsystems and components to provide an enabled environment for smooth operations and connectivity of mobile devices and information systems. Therefore, security of mobile device needs to be addressed at different layers (subsystems and components) of the mobile ecosystem. Wireless networks are key to most mobile products today. It is also essential to offer a variety of user experiences and features, primarily in the form of applications (email, browsing, gaming, social accounts, etc.). In order to support such an ecosystem, a mobile device vendor works closely with network operators, enterprise systems, app developers and so on. The figure below offers more details.

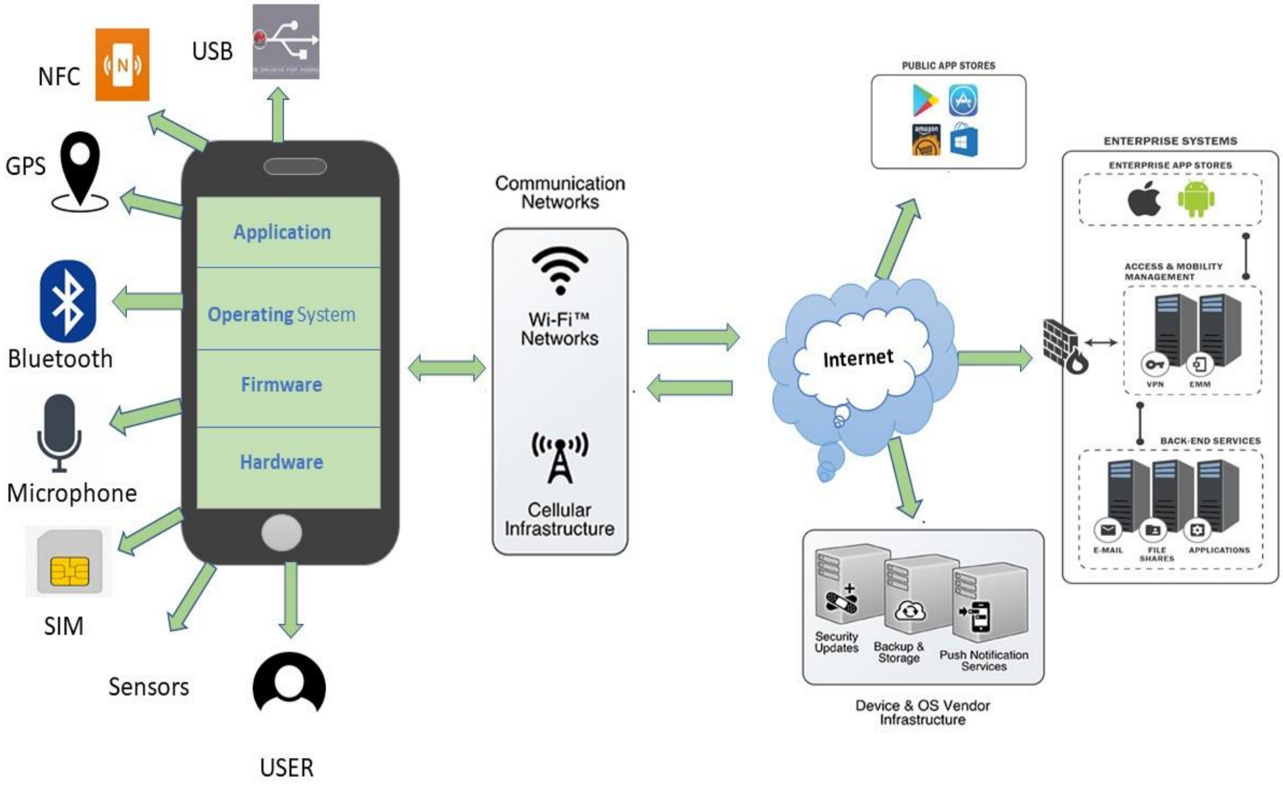

Fig II. Various components of Mobile Device Ecosystem. (Source Reference 9)

4.0 Threat Perception

Threat perception has drastically changed with the introduction of Mobile Operating Systems and innovations in Mobile Device Technology. Mobile Device Users began trusting their devices with enormous quantities of sensitive personal information/data. Enterprises also started allowing employees to use Mobile Devices and Applications to access their mail, contacts, calendar and data servers. This had drastically modified the attack surface. Rooted phones, Cloud services, Unsafe 3rd party applications coupled with advanced abilities of mobiles as well as increasing attack potential of cyber criminals made the mobile ecosystem more susceptible to attacks.

Security Threats to the Mobile Device (but not limited to): Malware, Malicious Applications, Mobile Device Integrity Compromise, Unauthorized Physical Access, Eavesdropping, Replay attack, Man in the Middle, Denial of Service, Loss of sensitive data, Unauthorised gathering of privacy and sensitive information, Exploitation of underlying vulnerabilities in OS and Firmware, exploiting access to enterprise network, Unauthorized Encryption of User data (Ransomware), Attempting to Rooting/jailbreaking of Mobile device, Manipulation of Trusted Applications, Exploitation of Application Stores. etc.

Security Threats to mobile device can be emanating from multiple sources, few are summarized as below,

1. Applications
    Malicious/Privacy Invasive Applications
    Vulnerable Applications
    Privilege Escalation to perform a malicious action
    Dynamic Code Execution

2. Physical Access
    USB Debug
    Malicious Charging Points

3. Mobile Device Technology Stack
    Mobile Operating System
    Device Drivers
    Trusted Execution Environment
    Boot Firmware
    Baseband Subsystem
    SIM Card
    Cryptographic Modules

4. Network Connectivity
    Cellular Access: GSM, CDMA, LTE, VoLTE, SS7.
    SMS, MMS, RCS, USSD.
    Wireless Network Access, LAN/PAN: WiFi, Bluetooth, NFC.

5. Ecosystem
    Application Stores: OS Vendor, Device Vendor, Private Enterprise Store, Third Party Stores

6. Enterprise Device Management
    MDM (Mobile Device Management)

7. Payment
    Financial, Payment, Banking Applications
    USSD Based /NFC Based Payments
    Payment Specific Threat

8. Software Management
    Software supply chain related threats
    Update/Upgrade/Patch Management

9. Authentication
    Local & Remote Authentication and Authorization

However, the security threats emanating from other components of mobile ecosystem such as third-party mobile applications, mobile network and infrastructure, Protocol inherent vulnerabilities, SIM are out of scope for this document.

5.0 Methodology of Mobile Device Security Testing

Mobile device security is a complex problem which requires coordinated effort from all stakeholders in order to provide essential security to the Device as well as data. Mobile Devices extensive mobility (portability), always on connectivity and associated complex ecosystem exponentially compounds the complexity of device security challenge thus requires a totally different approach & strategy to address Mobile Device security vis a vis normal computer systems and applications. Contemporary Mobile Operating Systems are different from Desktop/Laptop operating systems, and mobile applications are different from web applications.

“ONE SIZE FITS ALL” security strategy may not be sufficient in case of Mobile Device due to diversity in Mobile Platforms & Devices and varied security threat perception which may be varying from Device to Device (CEO of a MNC might be having altogether different threat level compared to Normal Employee or Common Citizen). As we understand security comes with cost, imposing threat perception of MNC’s CEO on common citizen does not appear rational. So, instead of single level security requirements for all Mobile Devices, this document has proposed Multi - Level of Security Testing Requirements. Advanced threat landscape, intention to minimize the disruption to existing mobile ecosystem and implication of Mobile device security testing to all stake holders are few other reasons for proposing Multi Level Security Testing.

There are two levels of security testing proposed in the present document. They are Level 1 and Level 2, with progressive increase in rigour of security testing from Level 1 to Level 2. Applicability of various Levels of security testing to the Mobile devices is mentioned in the below table.

Security Testing Level	**Applicable to Mobile Devices**
Level 1	All the Mobile Devices (Ownership Personal, Usage Personal)
Level 2	Mobile device used for both enterprise and personal use, where device owned/sponsored by enterprise/organization

Table 1

Security requirements for Level 1 security Testing will be applicable to all the mobile devices intended for personal usage and owned by person. Security requirements applicable for Level 1 security testing of Mobile Devices are placed at Section 6 of this document. Level 2 security requirements will be specific to meet the respective threat landscape and will be in addition to the security requirements mentioned in Level 1. They will be subsequently updated in Section 7.

For each mobile device, applicable security requirements for ‘Mobile Device security testing’ need to be determined by the Regulator based on the Mobile Device under evaluation. Required inputs/support for the same shall be provided by OEM.

6.0 Security Requirements for Level 1 Security Testing of Mobile Device

Section 6.1: Application Security

6.1.1 Application Signing before installation

Requirement:

All applications shall be digitally signed by the developers before they are installed in the device. Any attempt to install an application without developer’s signature (digital signature) shall be rejected by the Mobile Device. Application signing helps devices and users to identify the developers of the application and will ensure that the app has not been tampered post-signing.

All applications with invalid signature must be discarded by the Mobile Device. Hashing & DSC algorithms shall be in compliance with “Crypto Controls for ITSAR” notified by NCCS DoT complied hashing algorithms and secure key exchange algorithms.

6.1.2 Secure Application Update/Upgrade

Requirement:

Before installing update/upgrade to an application, Mobile Device has to verify the source authenticity using applications cryptographic key (Public key). Updates/Upgrades to an application shall be signed by the same cryptographic (Private key) used to sign the prior updates and the first version of the application. If update/ upgrade is not signed by same cryptographic (Private) key update to the application shall be discarded.

This process also assures developers that only they can update their own applications, and a malicious actor cannot push a rogue update to another developer’s application. Hashing & DSC algorithms shall be in compliance with “Crypto Controls for ITSAR” notified by NCCS DoT complied hashing algorithms and secure key exchange algorithms.

6.1.3 Banking/ Finance Application Verification

Requirement:

The mobile device platform shall support Certificate Authority (CA) application digital signing and verification, in addition to the digital self-signing mechanism /methodology. Sensitive pre-installed applications in the Mobile Device (Shipped along with Mobile Device), particularly related to (but not limited to) banking, finance, digital wallets and payment applications shall be signed using certificates issued by a Certificate Authority. This feature may also be used by third-party application developers to offer enhanced application verification of their apps by the end-user devices. Any application with invalid signature must be discarded by the Mobile Device.

6.1.4 Application Permissions

Requirement:

The permissions required by the application (for all applications i.e system/preinstalled/2nd party/3rd party ...etc) shall be explicitly produced for user’s approval. User shall have the option to allow/deny requested individual or all the permissions. Permissions shall be removed on successful removal of the app from the device and reinstallation shall prompt for permission approval again. Also, device must not grant any runtime permissions to preinstalled apps unless the user's consent is obtained before the application uses it (or preinstalled application is set as the default handler). The user shall be able to verify, add or remove permission at any time after initial installation and configuration.

The Mobile Device operating system shall ask users to explicitly grant permission (via a User Interface pop-up) when an application tries to access the resources that are not in its application sandbox. In order to educate the user about the permissions needed for the application to run services, the application framework shall provide application permission list upfront (via User Interface pop-up) to the user during installation or at runtime.

6.1.5 PII (Personally Identifiable Information) data non-disclosure

Requirement:

System applications and the other pre-installed apps (shipped along with Mobile Device) shall not store user personal data beyond what is required for its functionality. If the applications require to store such information, those shall not be stored in plain text or in public storage. PII may include (but not be limited to) passwords, PIN, access tokens, cookies, refresh tokens, cryptographic keys, financial data, user contacts, biometric information, and so on

Cryptographic Controls for ITSAR (as notified by NCCS, DoT) compliant encryption mechanism shall be used to encrypt sensitive PII data, if stored in public storage.

6.1.6 Access to device usage history and statistics

Requirement:

If device implementations include a pre-installed app or wish to allow third-party apps to access the usage statistics, those permissions shall be explicitly intimated to the user (with an option to deny) and shall get his approval for the same. There shall be a feature to grant or revoke access to the usage stats. PII shall not be collected in usage statistics.

6.1.7 Types of Applications and Privileges

Requirement:

Applications shipped along with mobile device shall have clear demarcation with regard to privileges and permissions. Applications shipped along with mobile device can be demarcated as System Applications, Pre-Installed OEM Applications and Pre-Installed 2rd Party Application. Privileged applications (System & Pre-Installed) shall be clearly indicated along with the permissions they have on sensitive user data. For, Pre-Installed 2nd party/Partner applications permissions refer Test Cases 6.1.4.

For all the privileged system and preinstalled application’s, the permissions granted on services and user data has to be listed down and there shall be valid justification for giving permissions on user sensitive data (if they needed so).

6.1.8 Restriction on Global Permission

Requirement:

Read and Write permission to the application sand box shall be with the concerned application itself or with privileged system application which has permission to do so. Package Manager / Service in the Mobile Device shall by default disable the Global Read and Global write permissions for application sandbox

6.1.9 Application Visibility

Requirement:

All the installed applications shall be visible/ accessible to the user in the Graphical User Interface/Home Screen/Settings → Applications. No Application shall be hidden or invisible to the user by default (Example: Spyware). All user installed and pre-installed 3rd party applications shall preferably be listed in Home Screen/GUI. Mobile device /Package manager shall provide an option to hide the application if User wishes to hide the application from home screen.

6.1.10 Permissions Related to User Privacy

Requirement:

Application seeking permission to access to Camera, Micro phone, Location Services, Phone and Contacts can only use the permissions when the application is in use. (i.e restriction on the background usage of Camera, Micro Phone and Location Permissions). User shall be notified if any application/service accessing/using the above said permissions in the background in the notification/status bar (continuous warning till the user addresses the same). The above permissions shall be denied when the applications are not running to avoid malicious usage/exploitation of permissions given.

Applications using above permissions shall clearly disclose the User regarding the same in fore ground. (For Example: status bar showing the applications/services using above mentioned permissions).

6.1.11 User consent policy for Advertisements

Requirement:

If device implementations include adding or pushing of items such as advertisements etc. then those shall be explicitly intimated to the user and ask for user consent before enabling the same.

6.1.12 Mobile Device Communication Policy

Requirement:

Any Communications of Chargeable or Non chargeable nature (such as SMS, MMS, Audio/Video Call …etc) shall not be initiated without explicit approval from the user for same.

Applications responsible for chargeable nature of communication shall not be allowed to run in the back ground without user permission.

Even after the user has consented to allow sending of such communication for a given application, it shall be possible to revoke such access and disallow the feature.

6.1.13 Inter APP Communication and Service Permission Enforcement

Requirement:

An application can be interacting with another application in Mobile device. Service calls shall be handled in a predefined manner in order to ensure that no unauthorized privilege escalation or no unauthorized usage of one application resource by another application

There shall be options for one application to be able to export its services to other applications in a secured manner. An application shall be able to enforce appropriate permissions to securely export its services. The device shall verify the permissions and exceptions shall be thrown if the caller does not have the required permission.

Permission checks are necessary when service level calls are made to start, stop, attach a service. An application shall be able to choose not to export any of its services to any other app.

6.1.14 Application and System events management

Requirement

Events triggered by a given application or system can be subscribed by other applications. There shall be option to enforce permission on whether an application can receive a particular system event or not, for sensitive contents.

Section 6.2: Vulnerable & Malicious Application

6.2.1. Application White Listing

Requirement:

Device Manufacturer/OS Developer App Store shall maintain a database of harmful apps (By means of Application Whitelisting and Black Listing Every App Store such as Apple Store or Google Play store/OEM/Mobile Device Manufacturer App Store shall maintain the list of blacklisted applications). Prior to installation, Mobile devices shall be able to identify the white listed application and allow the installation of only white listed applications.

By default, Mobile device shall disable the installation of applications from untrusted sources. User shall be able to enable the same if he requires. But mobile device shall display the suitable warning indicating the implications of the action (i.e. enabling installation of applications from untrusted sources).

6.2.2. Potentially Harmful Applications

Requirement:

Device shall check whether any known potentially harmful applications are installed in the Mobile Device. There shall be periodic monitoring in this regard and identified potentially harmful applications (for example: applications with multiple permissions) shall be intimated to user via visual means with an option to uninstall/discard.

Device shall also prevent installation of applications from within a running application or installing application without users' consent.

Device shall support Malicious Code protection (Anti Malware Software with periodic update (i.e at least once in 3 months). It shall alert the user when user tries to install an app that might be harmful and block the installation of harmful application.

6.2.3 Vulnerable Applications (Optional)

Requirement

System and the pre-installed apps (Pre-Loaded/Bundled/Stock/Partner/Pre-Installed applications shipped along with Mobile Device) shall be free from known vulnerabilities and software defects listed in OWASP Top Ten and any other standards as prescribed by NCCS. OWASP MASVS L1 v1.1 or Latest Version (OWASP Mobile App Security Verification Standard v1.1) based security testing desirable for all the System and preinstalled applications (shipped along with Mobile Device). It is desirable to have OWASP MASVS L2 - R v1.1 (or latest version) based security testing done for applications (Pre- Laded/Bundled/Stock/Partner/PreInstalled) handling sensitive finance related data such as banking, finance, digital wallets and payment applications.

6.2.4 Known Malware

Requirement:

Mobile Device shall provide service for known malware detection and protection. It shall scan the devices periodically to identify the known malware to protect the user data. The Detection service can throw a pop up to the user for each malware detection incident and if required shall block the malware.
The service has to be privacy preserving intrusion detection system to track and mitigate known security threats in addition to identifying new security threats. This feature shall to be provided by Mobile Device Vendor by default. Security Updates for this feature shall be available for every 3 months (for a period of minimum 3 years from release date of the mobile in to market) in order to update the malware signature database periodically to effectively tackle emerging threats.

6.2.5 Privacy Intrusive Applications

Requirement:

The Mobile device platform shall provide a service to detect malicious activity of the installed applications (can be part of device activity manager). The Detection service can throw a pop up to the user alerting the malicious activity and if required shall block the application responsible for malicious activity.

(For Example: One application trying to access information from other application's sand box or system resources which it is not authorized to access)

Protections against data leaks shall be implemented. Monitoring and controlling communications at the external boundary of the system as well as at key internal boundaries within the system shall be enforced.

Section 6.3: Application Isolation

6.3.1 Isolation of System apps

Requirement:

System apps shall not run with shared system UID with any other Partner/2nd Party/3rd Party/ Pre-Installed Application to avoid unintended privilege escalation thus endangering user's privacy. Privileged process IDs/System process IDs (Reserved user identifiers) shall not be used by any pre-installed/2nd party/3rd party/ applications except system applications.

6.3.2 Application Sandboxing

Requirement:

Sandboxing: OS or Application level mechanism utilizing multiple protection, isolation and integrity capabilities to achieve higher levels of overall isolation.

Mobile Device shall assign a unique user ID (UID) to each application and runs that user in a separate process. Operating System shall enforce isolation between applications at the process level in order to prevent data leakage between applications.

Mobile device shall also provide application isolation solution, such as a secure containerization to provide application level encryption. Such Application Data shall be accessible to only authorized users and services. With secured containers Application Data is protected during storage, processing and even in the case of loss of mobile device.

6.3.3 Sensitive User Data Security & Encryption

Requirement:

Data belonging to the pre-installed applications that collect, process and store sensitive user data and PII shall be encrypted while at rest and also during transmission. Sensitive user data and PII may include (but not be limited to) passwords, PIN, access tokens, cookies, refresh tokens, cryptographic keys, financial data, user contacts, biometric information, and so on.

Section 6.4: Mobile Device Data Integrity

6.4.1 Key Management service

Requirement:

The device software/hardware shall provide a key management service provider, which shall meet the following requirements:

1. The key management service shall provide user with options to generate keys/key pair and store in secure storage.
2. The key management service shall protect key material from unauthorized use by preventing extraction of the key material from the device and application processes.
3. The key management service shall enforce user authentication for key use and the keys shall become permanently invalidated once the authentication is disabled or forcibly reset (e.g. by a Device Administrator).
4. The key management service shall allow Import of encrypted keys securely
5. Keys shall be automatically removed from the system after deleting the application.

Above mentioned provisions are in conformance with FIPS 140-2 (or above) as prescribed by NIST standards.

6.4.2 Trusted Credential Storage and Management

Requirement:

The system certificate store shall include all CA-signed certificates for use by applications (pre-installed and commonly used third-party apps such as browsers etc.). Application specific certificates and certificates not signed by globally recognized Certificate Authorities shall be included only within the components/apps that need to trust them.

When a new certificate is required to be added to the system certificate store, or an existing certificate in the certificate store is modified or removed, the mobile device shall prompt the user to present authentication attribute (such as Pin/Password) to allow such an operation. If not configured to use such an authentication mechanism, the device shall not allow the addition or modification of the system certificates.

Device shall warn the user, via visual means, whenever a user certificate is installed. Device shall not allow a user to add system level trusted certificates.

6.4.3 Cryptography Requirements

To ensure usage of strong cryptographic encryption/decryption/hashing/MAC algorithms.

Requirement:

There shall be software cryptographic implementation support in the device which includes only the strong and recommended algorithms in compliance Cryptographic Controls for ITSAR (as notified by NCCS, DoT) publication.

It is desirable to use tamper resistant hardware for performing Cryptographic Operations and for secure storage of credentials.

Algorithms related to Radio Access or Baseband Standards such as GSM, UMTS, LTE, LTE A, …etc finalized by 3GPP/ITU/Global Standard Bodies… etc shall be allowed. The specified requirements are w.r.t data storage/processing/transit of Mobile Applications/User.

Section 6.5: Mobile Device Data Protection

6.5.1. Mobile Device encryption

Requirement:

Mobile Device Operating System shall provide Cryptographic protection of all or portions of a device's data storage locations - primarily flash memory locations. Cryptographic Controls for ITSAR (as notified by NCCS, DoT) compliant mechanism shall be used to secure data in storage. Cryptographic key used to encrypt the flash memory locations shall be encrypted using user device authentication attribute and stored in secure storage location.

6.5.2 SIM (Subscriber Identity Module) card lock

Requirement:
Mobile Device encryption doesn’t provide any protection to the SIM card. Device shall provide an option to the device users to lock the SIM card with authentication attribute. It prevents the malicious usage of the SIM card when an attacker removes the card and tries to use it on an unauthorized phone.

6.5.3 Secure storage

Requirement:

The device shall offer a secure storage solution that uses hardware/software-based mechanisms to protect the data. Read and write operations to such storage shall be restricted to authorized services and applications only (for example, Android Key store/Apple secure Enclave).

The following rules shall apply:

(1) Applications may be able to store secret/sensitive and confidential data in the secure storage through a privileged service. Each application shall have access (read and write) to its own sensitive information
(2) Malicious application running with elevated privileges shall not be able to read/write arbitrary keys in the secure storage

It is desirable to implement the secure storage feature via a Trusted Execution Environment (TEE) or through a dedicated hardware module.

6.5.4 Memory Isolation

Requirement:
One Process shall not be able to access or modify another processes memory. OS level capability shall be provided by mobile OS.

Section 6.6: Secure Physical Access & Secure Mobile Device Debug Options

6.6.1 Access to Developer Mode

Requirement:

If the Mobile Device supports enabling of end user to access advanced OS features/Kernel Access/Custom Boot Options, then those additional options shall be reasonably protected from accidental abuse. Developer mode shall not be easily accessible to the user, to avoid the accidental enabling of Mobile Device debug mode. For example, by default android tries to make ADB access harder by requiring you to use a “secret knock” (usually, tapping the build number seven times) in order to enable it. Developer options shall not be enabled by default.

Turning on Mobile Device debugging allows enhanced access to the device interfaces, data and debugging privileges on the mobile device. Mobile Device debugging option shall be disabled by default and if enabled and not been used for 1 hour it shall be disabled automatically.

6.6.2. Secure Debugging

Requirement:

Secure port (USB/Lightning/other) debugging shall be implemented such that only certain hosts, which are explicitly authorized by the user, are able to access the debug mode on Mobile Device to execute debugging commands. Thus, if someone tries to connect a mobile device to another host via debug port in order to access debug mode, they shall be prompted for authentication attribute. (i.e they must first unlock the target device and authenticate the access)

The Debug mode host authentication functionality shall be enabled by default by OEM and it shall not be possible to disable it via the system interface.

In secure debug mode device shall mandate the verification of cryptographic keys supplied by the requesting host, before allowing access to debug.

6.6.3 Secure storage for Debug authentication Keys

Requirement:

If mobile device supports any debug service like USB Debugging, Debug authentication keys shall be stored securely and owned by the SYSTEM UID. Permissions of the key storage shall be such that they're only readable (by applications which has permission to read) and not modifiable by unprivileged third-party applications.

6.6.4 Unused Physical Interfaces Disabling

Requirement:

The Mobile device shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces which are not under use shall be permanently disabled so that they remain inactive even in the event of a reboot. Such physical interfaces include USB, Lightning, UART, JTAG… etc. USB/Lightning is often used for charging and data transfer on most mobile devices, but there may be some classes of devices that expect users to use the USB interface only for charging. Data transfer over USB shall not be allowed on such mobile devices.

The system requirements shall clearly indicate the expected use of physical interfaces.

Note: List of the Physical Interfaces/Ports as given by the vendor shall match the list of Physical Interfaces/Ports that are necessary for the operation of the Mobile device. JTAG interface shall be disabled by default.

Section 6.7: Baseband & Communication Modules Isolation and Integrity

The baseband processor is the subsystem of the mobile device that controls radio communications. Baseband processor is a chipset on the phone that directly controls cellular hardware and communications with cell towers.

6.7.1 Baseband & Communication Modules Isolation

Baseband activities to manage network connections which include the cellular and Wi-Fi baseband, the NFC subsystem and others shall be isolated from main processor that runs the device’s primary operating system and SIM. It is desirable to have dedicated hardware-based baseband implementation for Baseband related activities in order to isolate these from the main processor/OS.

6.7.2 Baseband System Integrity Check

Mobile device shall have well defined integrity checking mechanisms to verify the Baseband Subsystem during Boot up/power on. Integrity checking mechanisms shall verify software, firmware, and information files integrity of Baseband System on every boot up/power on.

Section 6.8: Multi Physical User Support – Data Protection

6.8.1 Isolation of User’s Data

If the mobile device supports multi physical user per device, there shall be isolation of data belonging to each user at application as well as system level.

Requirement:

1. Device shall have separate and isolated shared application storage (in device’s public storage) directories for each user.
2. Device shall ensure that applications owned by and running on behalf a given user cannot list, read, or write to the files owned by any other user, even if the data of both users are stored on the same volume or file system.

Device shall encrypt the contents of the internal memory belonging to other user when multi user is enabled using a key stored only on non-removable media accessible only to the system.

Section 6.9: Mobile Device Operating System Security

6.9.1 Security Hardened Operating System

Requirement:

The mobile device shall use a hardened operating system (for example, SELinux for Linux-based operating systems, Mandatory Integrity Control for Windows platforms, etc) for all its applications and services. Such a hardened OS shall support Mandatory Access Control (MAC) measures in addition to the commonly-used Discretionary Access Control (DAC) mechanisms. The purpose is to be able to define and deploy fine-grained access control measures for vendor and third-party supplied software executing on the client devices.

Specifically:

1. The hardened OS shall not only monitor but also deny anomalous activities
2. The vendor may choose to add new rules and restrictions to enhance the security of the platform

It is desirable for the Mobile Device Operating system to follow secure configuration practices, based on Centre for Internet Security (CIS) Bench Marks, SANS Mobile device Security Check List and other standards as prescribed by NCCS.

Note 1: Selection of CIS benchmark if used shall be based on the OS version available on the Mobile Device to be evaluated, Ref: CIS Benchmarks for Android and iOS.

Note 2: Selection of SANS Mobile Device Security Check list shall be based on the OS/ Firmware supported by Mobile Device

6.9.2 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems

6.9.3 Growing Content Handling

Requirement:

Growing or dynamic content (e.g. log files, media files, or any other file) shall not influence system functions. Internal memory or RAM or device resources that reach its maximum capacity shall not stop a system from functioning in intended way. Therefore, countermeasures shall be kept in place such as memory monitoring and inform the user the source (like either the SD card was overloaded or an application sand box…etc) to ensure that this scenario is avoided.

Mobile Device Operating System shall provide features for device resource management for optimal and efficient usage of available resources.

6.9.4 Device Tamper Detection

Requirement:
Mobile device/OEM shall possess the capability to identify whether Rooting or jail breaking or act of similar sort occurred in the device and shall be intimated to the User. The same shall be notified to the user via visual means (by means of continuous warning banner which needed user action to close it) and recommend corrective measures. Rooting and Jail breaking of Mobile device may indicate that security architecture for the mobile device has been compromised.

Section 6.10: Mobile Device Boot Security

6.10.1 Hardware-backed Verified Boot

The Mobile device shall verify the integrity of the software stack (firmware and operating system, up to the system partition) using a hardware Root of Trust (RoT). This code, and related data is protected even when the device is powered off. This verification shall be performed via a cryptographic signature verification process. The verification key (or the hash of it) shall be integrity-protected and shall be stored in a memory location that cannot be tampered (secure storage or a read-only memory location). The mobile device shall verify the software/firmware image integrity at boot time, detecting, for example, software and firmware tampering and/or unauthorized software/firmware image updates.

The recommended cryptographic algorithm shall be Cryptographic Controls for ITSAR (as notified by NCCS, DoT) compliant for signature verification.

6.10.2 Trusted Execution Environment

Requirement:

Trusted Execution Environment (TEE) is a protective environment that runs a secure OS in the main processor of Mobile Device. TEE includes Key Storage and Management Functionalities (conform to ISO 11568- Secure Management of Cryptographic Keys). TEE also includes secure storage, which can be used to store transactional logs and authentication credentials in a private area. TEE (on Android and Other Devices) and Secure Enclave (on Apple iOS Devices) runs independently of main operating system. Mobile Device shall support TEE for secure storage/secure applications execution/cryptographic operations …etc.

6.10.3 Restricting System Boot Source

Requirement:

The Mobile device shall boot from the specific memory location allocated for the device to boot. Usually this refers to the OS, firmware and binaries stored on the device embedded Multi-Media Controller (eMMC) or the local flash. External memory devices (such as SD cards) shall not be used to boot the mobile device.

Section 6.11 Mobile Device Software/Firmware Update

6.11.1 Anti-Roll Back (ARB)

Requirement:

The Mobile device shall store the minimum secure version of the platform firmware at a secure memory location. The device shall not allow installation of a firmware whose version is older than that minimum secure version, even if it is validly signed by the OEM/ODM and can clear the verified boot checks successfully. For example this is also available via ‘Version Binding’ feature of Android.

The device manufacturer shall define the minimum secure version of the platform firmware and optionally update the field in secure storage during a firmware update cycle.

6.11.2 Secure Firmware Updates & Secure OS Update

Requirement:

All firmware and software updates for the mobile device, supported through over-the-air or via tethered channels, shall be integrity-verified using a cryptographic signature verification process. This check shall be performed before the newly downloaded image is copied over to the memory of the mobile device. Upon the successful cryptographic verification and copy of the image to the memory of the mobile device, the device shall reboot and go through the hardware-backed verified boot process. The protective hardware provides a trusted execution environment (TEE) for the privileged code to run and protect their code and data. Firmware/OS update and native firmware/OS shall use the same manufacturer’s key pair to ensure the authenticity of source.

The recommended cryptographic algorithm for signature verification shall be Cryptographic Controls for ITSAR (as notified by NCCS, DoT) standard compliant.

6.11.3 Updates/Upgrade/Patch Management

Requirement:

All firmware and software updates for the mobile device supported through over-the-air or via tethered channels shall follow the following,

1. Major/Potential/High Risk security vulnerabilities found/ reported in respect of OS/Firmware/ Software/Preinstalled Applications shall be patched at the earliest.

2. Security Patches for the OS/Firmware/Software for all publicly known vulnerabilities shall be done periodically, i.e at least once per every quarter/3months for a minimum period of 3 years after release of the Mobile Device in to the market (Release date as notified to NCCS/DoT).

3. Duration of support for update/upgrade/security incidents related to Mobile Device shall be intimated to the user explicitly at the time of purchase.

4. All the major updates/upgrades/security patches shall be intimated to the NCCS before releasing in to market. Security testing of the same will be decided by NCCS on case by case basis.

5. Security Patch/Update for known vulnerabilities (severe) shall be made available to the end users with in stipulated time frame as and when requested by NCCS.

6. OEM/ODM shall be responsible for the update/upgrade/patch management of any 3rd Party software/ preinstalled or 2nd party applications associated with Mobile Device (where ever applicable)

6.11.4 Security for Recovery Operating System (ROS)

Requirement:

The Recovery OS is a minimal software stack used for performing system management tasks, install new firmware and recover the mobile device if the main operating system leaves the system in an inconsistent state.

The Recovery OS image shall be signed with the same manufacturer's keys that are used to sign the primary Board Support Package (BSP) and the platform firmware. Under normal operations where the boot loader is locked, the mobile device shall not permit the booting of a recovery OS which is not signed, or is corrupted

Section 6.12: Software Security

6.12.1. Publicly known security vulnerabilities

Requirements:

At the time of providing the mobile device to the Security Testing Facility the mobile device shall not contain any software or firmware with publicly known vulnerabilities. This is applicable to open source and proprietary/third-party software bundled with the mobile platform. Examples include security vulnerabilities in Open SSL, Bluetooth drivers/firmware, Linux kernel, etc. Vendors can refer to the sources such as NVD Database <https://nvd.nist.gov/>, CWE Top 100, OWASP Mobile Top 10 as a reference to check for publicly reported vulnerabilities in their software stack

6.12.2 Insecure Network Services shall be disabled

Requirement:

The Mobile device shall only run network protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. All deprecated services (deprecated protocols/applications) shall be permanently disabled and during reboot they shall not be revoked.

List of deprecated services (list is not exhaustive) FTP, TFTP, Telnet, rlogin, RCP, RSH, HTTP, SNMPv1 and v2, SSHv1 …etc

6.12.3 Secure Time Synchronization

Requirement:

Mobile device shall not allow third-party or vendor pre-installed applications to change the system time. There may be many aspects of security that can rely on the current system time, such as certificate expiration, license management, etc. Only privileged applications (such as system apps) shall be allowed to modify the system time.

Also, network time Synchronization shall be from secure NTP server and shall be over TLS (Latest Version) or as prescribed by NCCS.

6.12.4 Remove unsupported and outdated components

Requirement:

The Mobile device shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end-of-life or end-of-support, applications that are no longer maintained, or those which are vulnerable/ compromised. All the software and hardware Components shall have support contract with the OEM/Producer/Developer. This support contract shall guarantee the correction of vulnerabilities over components' lifetime.

Section 6.13: Communication Security

6.13.1 Secure Wi-Fi EAP, VPN Credentials Management

Requirement:

If a TLS or Wi-Fi credentials are stored in insecure location, attacker's application can read the credentials and send it to attacker server. Attacker can then read all the communication from the device using the credentials. In the case of both EAP-TLS and PKI-based VPNs, clients have an authentication key and are issued a matching certificate and these shall be stored in the secure location. (It is desirable to store such credentials at system credential store).

6.13.2 Proper Host-based card emulation (HCE) in NFC

Requirement:

The card emulation mode may rely solely on the OS to enforce security. If so, OS shall implement proper security policies for the same.
HCE service shall be protected by system permission, so that only the OS can bind to and communicate with your service. This ensures that any APDU you receive is actually an APDU that was received by the OS from the NFC controller, and that any APDU you send back will

6.13.3 Securing listening network sockets

Requirements:

Sockets are heavily utilized by the native layer of the OS at runtime. Exposed Inter Process Communications channels, if not properly protected, could be abused by adversaries to exploit vulnerabilities within privileged system daemons and the kernel. Other than the system, applications also have access to IPCs.

Root or Privileged SYSTEM UID processes shall not listen to any port on the Mobile device. Any system UID listening on any port shall be intimated to the user

Services and daemons that handle listening ports must be robust and shall protect against malformed data.

Section 6.14: Regulatory Features

6.14.1 Panic Button & GPS

Requirement:

All the Mobile devices shall have the Satellite based GPS facility and Panic Button facility as mandated by regulator. All the Mobile Devices shall provide the “Panic Button” feature as required by the regulator. “Panic Button” feature shall enable the device user to communicate to Law Enforcement Authority in case of emergency

6.14.2 Geo Fencing

Requirement:

Tracking mobile device and trigger an event/alert – stop services when boundaries are crossed. Mobile device shall be able to create & monitor Geo fences: The use of GPS or RFID technology to create a virtual geographic boundary enabling software to trigger a response when a mobile device enters or leaves a particular area.

6.14.3 Simplified and user-friendly Privacy Policy

Requirement:

Mobile Device shall intimate the owners regarding the privacy implications of certain device and application functionality during device management setup/ device setup Implemented via privacy policy presented to users. i.e the ability to display a warning banner that a user must accept before gaining access. (Warning banner shall be short and crisp. Any information regarding collection of usage statistics and user information/data shall be clearly indicated in the banner itself in highlighted text). As an alternative, redirect users to an organizational website containing a sample privacy policy.

OEM/ODM/Mobile Device OS Provider shall adhere to the privacy policy published on the Device/Website/Public Domain and the same has to be submitted to NCCS at the time of submission of Mobile device for security testing. Any deviation/change of policy must be intimated to NCCS as well as User before the actual change comes in to effect.

6.14.4 Non-disclosure of user information on a locked screen

Requirement:

Mobile device shall provide an option to user to not to show the messages or any notification information when phone is locked. In this way, users can protect the sensitive data even if someone tries to steal data when phone is locked. And also, by default contents of the notification shall be hidden.

6.14.5 Unique Identification of Mobile Device

Requirement:

Mobile device shall contain a unique identifier which may be used to declare its identity for obtaining services from Access Network (such as International Mobile Equipment Identifier for 3GPP Mobiles). This unique identifier shall be intimated to NCCS/DoT by the OEM at the time of submission for testing.

Section 6.15: Secure Logging and User Audit

6.15.1 Audit Event Generation

Requirement:

The Mobile device shall log all important Security events with unique System Reference such as Application Name & UID, Hostname, Process ID, IP Address/MAC Address in case of remote operation … etc. These events shall also be captured in an Audit/log file stored in non-volatile memory (on the device flash). The Mobile device shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, and the result of the event (Success/Failure).
Logs shall be stored for Minimum 12 Months. The duration of retention of the logs on the mobile device and the maximum size of the logs shall be determined by the OEM and they shall comply with the regulations stipulated by the NCCS from time to time regarding the same.

Security events for which logging shall be enabled (but not limited to) are mentioned in Table below

Event Type	Description	Data to be logged (but not limited to)
Application Installation /Uninstallation/ Update	Keeps a record of Applications Installed/Uninstalled/ Updated	User Identity, Source, Outcome of Event (Success/ Failure), Time Stamp, Subject Identity, App Name/ID/ Version,

Installation of apps through unsupported channels (side-loading, unofficial App repositories, etc.)	Keeps a record of Applications Installed/Uninstalled/ Updated from unsupported channels	User Identity, Source, Outcome of Event (Success/ Failure), Time Stamp, Subject Identity, App Name/ID/ Version,
Installation and uninstallation of Device Manager and Mobile Device Management (MDM) Applications	Keep a record on MDM installation /uninstallation	User Identity, Source, Outcome of Event (Success/ Failure), Time Stamp, Subject Identity, App Name/ID/ Version,
Incorrect Login Attempt	Records any user incorrect login attempts to the MT	Username, Source (IP address, if remote access), Outcome of event (Success or failure), Timestamp,
Installation and uninstallation of system certificates	To record on the changes made to System Certificate Store	User Identity, Source (IP Address, In case of Remote access), Outcome of Event (Success/ Failure), Time Stamp, Subject Identity
Factory reset and erasure of user data in Mobile Device	To record the modifications to user data especially regarding Factory Reset	User Identity, Source (IP Address in case of remote access), Outcome of Event (Success/ Failure), Time Stamp, Subject Identity
Enabling developer debug access	To keep a record on Developer debug mode access	User Identity, Source (IP Address in case of remote access) Outcome of Event (Success/ Failure), Time Stamp, Subject Identity
Resource Usage	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded, Value reached (Here suitable threshold values shall be defined depending on the individual system.), Outcome of event (Success or failure), Timestamp
Configuration/Settings change	Changes to configuration/settings of the mobile device	Change made, Timestamp Outcome of event (Success or failure), Username
Reboot/shutdown/crash	This event records any action on the mobile device that forces a reboot or shutdown OR where the mobile device has crashed	Action performed (reboot, shutdown, etc.) , Username (for intentional actions), Outcome of event (Success or failure), Timestamp

Setting/Resetting Authentication Attribute	Creation/ Modifying Authentication Attribute. Removal or update of security access mechanisms (for example, removing the password, PIN, or biometric screen lock to allow for unrestricted access)	Activity performed (creation, delete, enable and disable), User Name, Outcome of event (Success or failure), Timestamp
Application Permissions	Starting and Stopping of Permissions to Services/Broadcasts/Intents … etc	Service identity, Activity performed (start, stop, etc.), Timestamp, Outcome of event (Success or failure), User Identity
User login	All use of identification and authentication mechanism	user identity, origin of attempt (IP address if remote access), Timestamp, outcome of event (Success or failure)
Secure Update	attempt to initiate manual update, initiation of update, completion of update (OS)	user identity, Timestamp, Outcome of event (Success or failure), Activity performed
Time change	Change in time settings	old value of time, new value of time, Timestamp, origin of attempt to change time (IP address in case of remote login), outcome of event (Success or failure), user identity
Audit data changes	Changes to audit data including deletion of audit data/log	Timestamp, Type of event (audit data deletion, audit data modification), Outcome of event (Success or failure), user identity, origin of attempt (e.g IP address in case of remote login), Details of data deleted or modified

The above list is also in compliance with the events described in 3GPP 33117 (to the extent possible)

6.15.2 Audit trail storage and protection

Requirement:

The security event log shall be recorded and can be accessed only by system/supervisor level user. System or application log files preferably be stored in secure storage. If they are to be stored in public storage, shall be stored encrypted (Cryptographic Controls for ITSAR (as notified by NCCS, DoT) Compliant Encryption). When logs of security-critical events are not stored in a secure location, attacker can modify the logs resulting in different outcome while finding the source of the attack.

System logs shall not be accessible to third-party applications (including pre-installed/ 2nd party/ 3rd Party Applications). Here, Logs will include both system event logs as well operational /application event logs. System user is allowed only to access the logs but not allowed to delete all logs.

6.15.3 Secure logging / debugging

Requirement:

The log entries shall not include messages with privacy-related information such as e-mail addresses, passwords, contact information, SMS/MMS, One Time Passwords, Financial Information, Credit/Debit Card Information.…etc. The preinstalled or system applications shall not log any sensitive/PII information.

Section 6.16: MDM (Mobile Device Management)

6.16.1 Proper MDM access rights

Requirement:

All restrictions on installing applications shall also be enforced to MDM app. The MDM admin shall possess only the access rights approved by the user as per the access control policies. Also, the MDM can be given administrator access only with user consent but cannot be given the root access to the mobile device.

6.16.2 User privacy and data separation

Requirement:

The mobile device shall enforce the MDM application to create and use its own container to isolate business data (like corporate emails, corporate documents on devices) and personal data. The MDM application shall not be able to access user's personal data such as photos, videos, email, location etc.

6.16.3 Access to other applications data

Requirement:

The mobile device shall not give MDM, access to data belonging to other applications installed in the device unless it asked for and was granted by user. It shall not be able to modify or delete the data belonging to other applications unless authorized. It shall not be able to install or remove any non-authorized applications/processes.

Section 6.17 Vulnerability Analysis, Penetration Testing & Source Code Review Requirements

Requirement:

The vendor shall perform complete security assessment, Source Code Review/Analysis, vulnerability analysis, penetration testing and fuzzing (for robust implementation) on all OEM-developed components on the mobile system. In order to ascertain the claims and ensure security assurance Test Labs will conduct the Source Code Review/Analysis, vulnerability analysis, penetration testing and fuzzing.

The OEM shall provide documentary evidence (Including Test Reports) as well as required inputs including source code to review the full Security Development Lifecycle (security architecture reviews, threat modelling, source code reviews, penetration testing and fuzzing) specific to the mobile platform.

Section 6.18: Authentication and Authorization

6.18.1 Local User authentication to Device

Requirement:

The various user accounts on the mobile device shall be protected from misuse/unauthorized access. The mobile device shall support use of an authentication attribute for local access, which enables unambiguous authentication and identification of the authorized user.

Authentication attributes include:
- Patterns (Minimum 3x3 dot matrix)
- PIN (Minimum 6 Numerals)
- Passwords (Refer section to 6.18.6)
- Biometric (Such as Fingerprint, Face Recognition, Iris Recognition, Retina Scan, Palm Scan)

Device shall support minimum two of the above attributes. Device can support dual factor authentications by combining 2 or more above combinations to provide higher level of security.

Mobile Device shall prompt for setting up authentication attribute for device access during initial boot up/setup.

6.18.2 Local User authentication to Applications

Requirement:

Applications on the mobile device shall be protected from misuse/unauthorized access. The mobile device shall support use of an authentication attribute for local access to the application, which enables unambiguous authentication and identification of the authorized user.

Authentication attributes include:
- Patterns (Minimum 3x3 dot matrix)
- PIN (Minimum 6 Numerals)
- Passwords (Refer to section 6.18.6)
- Biometric (Such as Fingerprint, Face Recognition, Retina Scan, Palm Scan)

Device shall support minimum two of the above attributes. Device can support dual factor authentications by combining 2 or more above combinations to provide higher level of security.

6.18.3. Remote Device/User authentication

Requirement:

The mobile device shall support use of an authentication attribute while accessing the device remotely for managing the device (for example, “Find my Device” for Android) to enable unambiguous authentication and identification of the authorized user.

For Remote Authentication, Authentication attributes shall include PIN/Password/Biometric Attribute and Web access tokens (or similar).

Remote access feature shall not be enabled by default (can be enabled in initial bootup/setup of the Mobile Device)

6.18.4. Protection against brute force and dictionary attacks

Requirement:

If a password is used as an authentication attribute, a protection against brute force and dictionary attacks that hinder password guessing shall be implemented. Brute force and dictionary attacks aim to use automated guessing to ascertain passwords for the mobile device. Various measures or a combination of these measures can be taken to prevent this.

The most commonly used protection measures are:

1. Using the timer delay for each newly entered password input following an incorrect entry ("tar pit"). Vendor may choose to implement the timer delay that could be the same or progressive increase (i.e increasing the lock out duration after certain incorrect attempts) depending the operator's policy for each failure attempt. The vendor shall define and implement the absolute limits for the number of incorrect attempts before lockout and the lockout duration.
2. Blocking an account following a specified number of incorrect attempts. The device shall allow the user to unblock the account and make the mobile device usable only after the user verifies his/her identity through an authorized cloud-based account or through a personal unblocking PIN (Minimum 6 Numerals)/ Password (Refer Test Case 1.4) (Different from user log in password) , which shall then allow the user to securely reset the access credentials to the mobile device.

Mobile device shall support at least one of the above two provisions.

6.18.5. Inactive session timeout

Requirement:

It shall be possible to configure an inactivity time-out period for a mobile device by the user. The inactivity time out period shall not be more than 30 Minutes. After expiry of inactivity time out period device shall prompt for authentication attribute.

Note: Inactivity time out period shall not be EVER

6.18.6. Strong Password support and Enforcement

Requirement:

OEM shall decide for an absolute minimum length which shall not be configurable by the user.

The mobile device shall only accept passwords that comply with the following complexity criteria:

1. Absolute minimum length of 6 characters (shorter lengths shall be rejected by the Mobile device). It shall not be possible setting this absolute minimum length to a lower value by configuration.
2. Password shall include combination of at least 2 categories mentioned below
    a. Uppercase character (A-Z)
    b. Lowercase character (a-z)
    c. Digit (0-9)
    d. Special character (e.g. @ ! $ / = * & # + -)

When a user is changing a password or entering a new password the mobile device shall check and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used.

6.18.7 Password Management Policy

Requirement:

If a password/PIN is used as an authentication attribute, then the mobile device shall offer a function that enables the user to change his password at any time.

Device shall not come with default user account and authentication attribute. At the 1st use/Initial Boot up/Setup, Mobile Device shall mandate the creation of user account with authentication attribute.

The mobile device shall enforce password change based on password management policy. In particular, the mobile device shall enforce password expiry. Password shall be expired in a predefined time (Eample:365 Days). Password expiry time is user configurable.

Password never expires option shall not be there.

Previously used passwords shall not be allowed up to a certain number (Password History). The number of disallowed previously used passwords shall be configurable and its default value shall be greater than or equal to 1.

This means that the mobile device shall store at least one previously set password. The maximum number of passwords that the mobile device can store for each user is up to the manufacturer. When a password is about to expire a password expiry notification shall be provided to the user and device shall insist on password change upon expiry of predefined password expiry time. Above requirements shall be applicable for all passwords.

6.18.8 Protected Authentication feedback

Requirement:

The Authentication attributes shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password/PIN are replaced by a character such as "*" before the next character is typed. Under certain circumstances it may be permissible for an individual character to be displayed briefly during input. Such a function is useful for device users due to small form factor of Mobile Device to make input easier. However, the entire password/PIN shall not be displayed in plaintext unless opted for the same by Device Owner.

6.18.9 No pre-existing physical (visible or hidden) user accounts

Requirement:

Mobile Device may ship with pre-installed applications which may have their own logical user accounts. However, the mobile devices shall not be configured with any default users and/or passwords, or PINs.

Creating such users and passwords may convey a false sense of security to end users. Users of the mobile platforms shall be required to create their own physical user accounts at first boot. The OEM shall not create or implement any such users, regardless of their visibility through the standard device users/accounts listing mechanisms.

OEM specific user with highest privileges shall not be created.

6.18.10. Protecting Confidential System Data

Requirement:

In Mobile device, the authentication attributes data (both device access authentication attributes and Application access authentication attributes) such as the PINs, passwords, biometric data (Fingerprints, Face recognition etc) etc shall be stored securely and not accessible to any unintended applications. Also, these confidential system internal data shall not be stored in clear text.

Cryptographic Controls for ITSAR (as notified by NCCS, DoT) standard compliant mechanism shall be used to encrypt sensitive data such as passwords, secret key, PIN, Biometric Authentication Vectors …Etc

7.0 Security Requirements for Level 2 Testing:

Will be notified subsequently

Annexure 1

Definitions

User Sensitive Data (shall include but not limited to)

Financial/Payment related Information, User Name and Authentication Attribute (Password/PIN/Biometric Information … etc), One Time Password, Contacts, SMS, MMS, Access and Refresh Tokens, Cryptographic Keys, Personally Identifiable Information, User Photos, User Videos and Audio Logs, Email, Credit/Debit Card Information and Passwords, IMEI ……. Etc

NCCS/DoT: National Centre for Communications Security, Department of Telecommunications, Ministry of Communications, Government of India or as prescribed by Department of Telecommunications

Preinstalled Applications: Pre-Loaded, Bundled, Stock, Partner, Pre-Installed applications shipped along with Mobile Device.

Annexure 2

Abbreviations

ACL - Access Control Lists
ADB – Android Debug Bridge
AOSP – Android Open Source Project
AES - Advanced Encryption Standard
API- Application Programming Interface
APDU – Application Protocol Date Unit
CA – Certification Authority
CERT-T - Computer emergency response team– Telecom
CVE - Common Vulnerabilities and Exposures
CWE - Common Weakness Enumeration
IPC – Inter Process Communication
USB – Universal Serial Bus
JTAG – Joint Test Action Group
UART – Universal Asynchronous Transmitter/Receiver
RoT- Root of Trust
TEE- Trusted Execution Environment
BSP – Board Support Package
RSA - Rivest–Shamir–Adleman(Algorithm)
OWASP – Open Web Application Security Project
SE Linux – Security Enhanced Linux
SEPolicy – Security Policy
TLS – Transport Layer Security
FTP – File Transfer Protocol
TFTP – Trivial FTP
Telnet – Teletype Network
rlogin – Remote Login Service
RCP - Remote Copy
RSH - Remote Shell
SNMP- Simple Network Management Protocol
TCP – Transmission Control Protocol

UDP – User Datagram Protocol
LLDP – Link Layer Discovery Protocol
DDOS - Distributed Denial of Service
NE - Network Element
NFC- Near Field Communications
FIPS - Federal Information Processing Standards
HTTP - Hypertext Transfer Protocol
HTTPS - Hypertext Transfer Protocol Secure
IPsec - Internet Protocol Security
VPN - Virtual Private Network
MD5 - Message Digest Algorithm
NTP - Network Time Protocol
OS - Operating System
IMEI - International Mobile Station Equipment Identity
ME - Mobile Equipment
MT – Mobile Device
OTA - Over-The-Air
SIM - Subscriber Identity Module
UE - User Equipment
PIN - Personal Identification Number
OEM - Original Equipment Manufacturer
ODM - Original Device Manufacturer
UID - User Unique Identifier
GID – Group Identifier
PII- Personally Identifiable Information
SMS - Short Messaging Service
MMS – Multimedia Messaging Service
API- Application Programming Interface
CA – Certification Authority
IPC – Inter Process Communication
USB – Universal Serial Bus
JTAG – Joint Test Action Group
UART – Universal Asynchronous Transmitter/Receiver
RoT- Root of Trust
TEE- Trusted Execution Environment
BSP – Board Support Package
RSA - Rivest–Shamir–Adleman(Algorithm)
OWASP – Open Web Application Security Project
SE Linux – Security Enhanced Linux
SEPolicy – Security Policy
TLS – Transport Layer Security

FTP – File Transfer Protocol
TFTP – Trivial FTP
Telnet – Teletype Network
rlogin – Remote Login Service
RCP - Remote Copy
RSH - Remote Shell
SNMP- Simple Network Management Protocol
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
LLDP – Link Layer Discovery Protocol;

Annexure 3

References

1) NIST Special Publication 1800-4b (Draft) - Mobile Device Security, Approach, Architecture, and Security Characteristics Cloud and Hybrid Builds

2) NIST Special Publication 800-124 Revision 1; Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013

3) NIST Special Publication 800-190 Application Container Security Guide September 2017

4) Draft NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations

5) NISTIR-8144 Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue, September 2016.

6) OWASP Top 10 Mobile Security Risks, 2016

7) OWASP MASVS, Version 1.1

8) CIS Benchmarks (Android and iOS)

9) Study on Mobile Device Security, Department of Homeland Security (DHS), April 2017

10) ISO 12812-1:2017 Core banking - Mobile Financial Services - Part 1 and Part 2: General Framework, March, 2017

11) ISO/IEC/IEEE 29119-1:2013 Software and systems engineering —Software testing — Part 1: Concepts and definitions

12) ISO/IEC/IEEE 29119-3:2013 Software and systems engineering —Software testing — Part 3: Test documentation

13) IEEE Std 610.12-1990 (R2002) IEEE Standard Glossary of Software Engineering Terminology

14) IS/ISO 31000- 2009 (reaffirmed 2011) Risk Management — Principles and Guidelines

15) National Institute of Standards and Technology, *National Vulnerability Database,* 2015. http://nvd.nist.gov

16) OWASP Mobile Security Testing Guide v1.1.3 2 August 2019

17) Protection Profile for Mobile Device Fundamentals by NIAP, 2013