Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

Operating system (OS)

(Draft for Comments)

ITSAR Number: ITSAR70101YYMM
ITSAR Name: NCCS/ITSAR/Miscellaneous/Operating System/Operating System (OS)

Date of Release: DD.MM.YYYY Version: 1.0.0
Date of Enforcement:

MTCTE के तहत जारी:
Issued under MTCTE by:

**राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत**

**National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India**

About NCCS

National Centre for Communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecommunication Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sr No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Operating System	ITSAR70101YYMM	1.0.0	DD.MM.YYYY	First release

Table of Contents

A. Outline

The objective of this document is to present comprehensive, country-specific security requirements for the operating system in telecom equipment. The specifications produced by various international standardization bodies/ associations like CIS, 3GPP, ETSI, IETF along with the country-specific security requirements are the basis for this document. This document contains a brief introduction, objectives, and security requirements for the OS running on the Telecom Equipment.

B. Scope

This document targets on the security requirements of the Operating System running on telecom equipment. It is applicable for Operating System running on all the telecom equipment.

C. Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of Indian Telecommunication Security Assurance Requirements (ITSAR).
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above

Chapter-1 Overview

1.1 Introduction

Operating system is essential software that manages computer hardware and provides a platform for running applications. In terms of security, they play a crucial role in protecting the operating system and its data from unauthorized access, malicious attacks, and other threats. There are several types of operating systems each designed for specific tasks and responsibilities, ranging from the highest to the lowest levels of the network hierarchy.

1. Network operating system (NOS): At the top level, network operating systems are used to manage and control the entire network infrastructure. They oversee the coordination of various network elements, such as routers, switches, and servers, to ensure data traffic flows smoothly and efficiently.
2. Carrier-Grade operating systems: Carrier-grade operating systems are designed to meet the stringent requirements of telecommunications carriers and service providers. These operating systems are highly reliable and capable of providing uninterrupted service, often with redundancy and failover mechanisms to minimize downtime.
3. Real-Time operating systems (RTOS): RTOS is essential for telecom equipment and devices that require precise timing and low-latency operation. These operating systems are used in applications like base stations, control systems, and data acquisition devices to ensure that critical tasks are executed with minimal delay.
4. Embedded operating systems: Embedded operating systems are utilized in telecom equipment and devices like modems, routers, and IoT (Internet of Things) devices. These operating systems are lightweight and designed to run on resource-constrained hardware while providing essential communication and management capabilities.
5. Hypervisors: Hypervisors are used to create virtual environments for applications and services. They enable efficient resource allocation and management, making it possible to run multiple virtualized instances of operating systems on a single physical server or device.
6. OS running on UEs: The OS running on the UEs is used to run end-user applications. They don’t have to be as light as IoT OSes or as heavy as server-grade. They are the most common form of OS.

These operating systems work together to provide reliable and efficient services at various levels of the network hierarchy, ensuring seamless data flow and communication to meet the needs of both consumers and businesses.

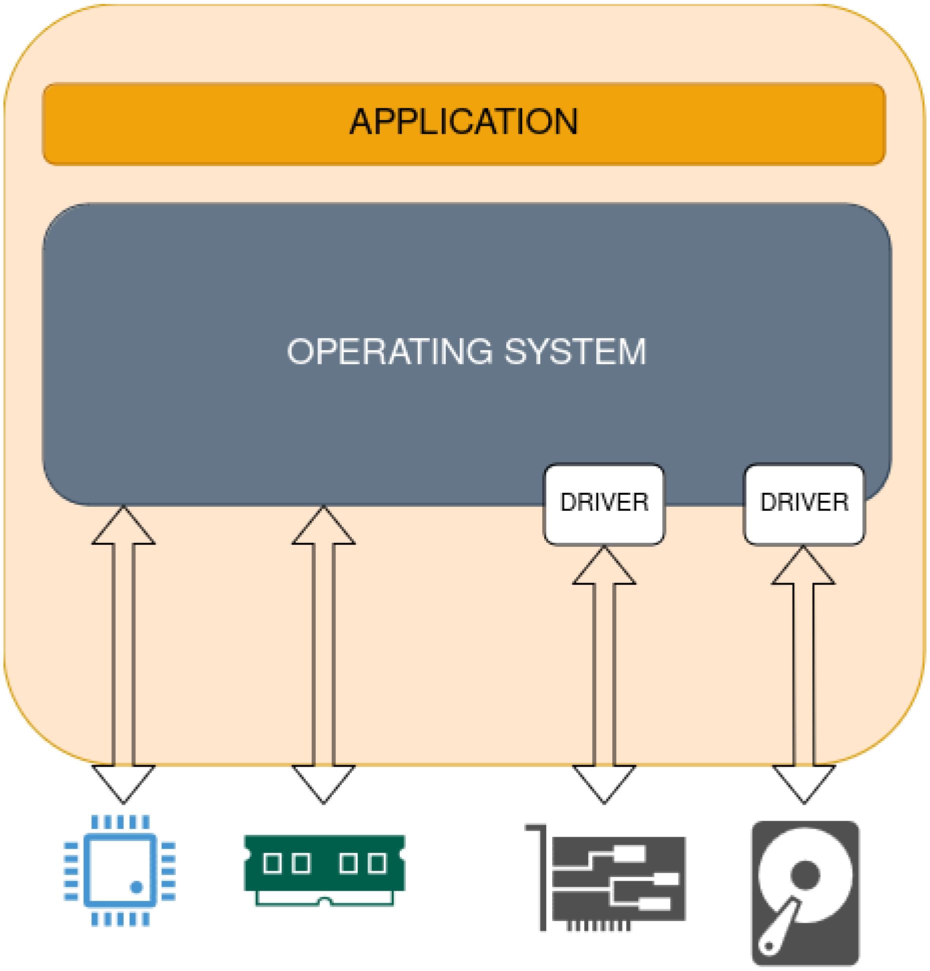

Figure1: Operating System overview

1.2 Hardware Overview:

Processors: Processors, also known as central processing units (CPUs), are the core components of a computer responsible for executing instructions and performing calculations. They interpret and execute instructions fetched from memory, enabling the computer to carry out tasks and run programs.

Memory: Memory, also referred to as RAM (random access memory), is a type of volatile storage used by a computer to temporarily store data and instructions that are actively being used or processed. It provides fast access to data for the CPU and other hardware components.

Non-volatile Storage: Non-volatile storage refers to persistent storage devices that retain data even when the computer is powered off. Examples include hard disk drives (HDDs), solid-state drives (SSDs), and flash memory. Non-volatile storage is used for storing operating systems, applications, user data, and other files.

I/O Devices: Input/output (I/O) devices are peripherals that allow users to interact with the computer and exchange data with the outside world. Examples include keyboards, mice, monitors, printers, scanners, network adapters, and storage devices. I/O devices enable input (data entry) and output (display or transfer of data) operations.

Buses: Buses are communication pathways or channels within a computer system that enable the transfer of data between various components, such as the CPU, memory, I/O devices, and storage devices. Buses consist of multiple electrical conductors or traces that carry data, addresses, and control signals.

The OS is responsible for managing all the above resources for the applications running above.

Booting the Computer: Booting the computer refers to the process of starting or initializing the computer's hardware components and loading the operating system into memory to prepare the system for use. It typically involves powering on the computer, performing a power-on self-test (POST), initializing hardware devices, loading the BIOS or UEFI firmware, and launching the operating system kernel.

1.3 OS Terminology:

Processes: Processes are instances of executing programs on a computer. They represent running tasks and consist of executable code, data, and system resources.

Address Spaces: Address spaces refer to the memory locations that a process can access. Each process has its own address space, which defines the range of memory addresses it can use. Trying to overcome this limitation is the purpose of buffer overflow attacks.

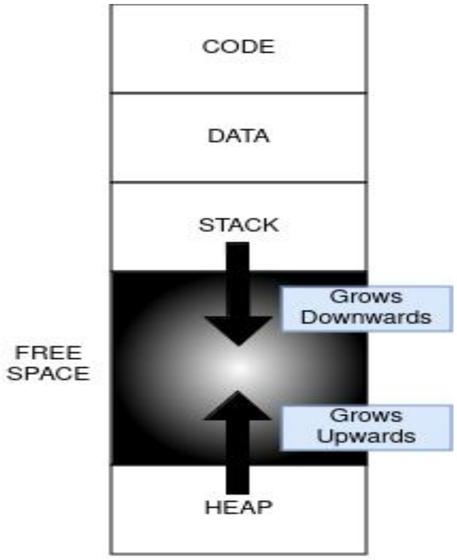

Figure 2: Process Structure

Files: Files are collections of data stored on a computer's storage device. They provide a way to organize and store information persistently, allowing users and programs to access and manipulate data.

Input/Output (I/O): Input/Output refers to the communication between a computer system and external devices. It involves transferring data to and from input/output devices such as keyboards, monitors, printers, and network connections.

Protection: Protection mechanisms in an operating system control access to system resources and ensure that one process cannot interfere with or corrupt the memory or data of another process.

The Shell: The shell is a command-line interface that allows users to interact with the operating system by typing commands. It interprets user commands and executes them by communicating with the kernel and other system components.

Kernel: The kernel serves as the central component of an operating system, responsible for handling essential tasks such as managing hardware resources, facilitating communication between hardware and software, and ensuring the smooth execution of processes. If you strip away all the UI and frontend of all operating systems, what is left is the kernel.

1.4 Operating System Structure:

User space and kernel space are two distinct areas of memory in an operating system, each serving different purposes and operating under different conditions. User space is where user applications and processes run. It has restricted access to system resources and hardware to ensure system stability and security. Applications in user space operate with low (non-privileged) permissions, meaning they cannot directly interact with hardware or access the memory of other processes or the kernel itself. When a user application needs to perform a task that requires higher privileges, such as accessing hardware or system resources, it must make a system call to request the kernel's services.

Kernel space, on the other hand, is reserved for the core components of the operating system, such as the kernel itself, device drivers, and system services. It operates with high (privileged) permissions, allowing it full access to all hardware and system resources. This privileged access enables the kernel to manage critical tasks like process scheduling, memory management, and hardware communication. Since the kernel operates in this highly privileged mode, any error or crash in kernel space can potentially bring down the entire operating system, whereas errors in user space typically only affect the individual application. This separation enhances overall system security and stability, ensuring that user applications run safely without risking the integrity of the entire operating system.

System calls: They are mechanisms that allow user-space applications to request services from the kernel, bridging the gap between user space and kernel space.

1. Request Initiation: When a user-space application needs to perform an operation that requires higher privileges (e.g., file access, process control, network communication), it initiates a system call.
2. Mode Switching: The system call triggers a switch from user mode to kernel mode. This switch is essential because it grants the requested operation higher privileges necessary for accessing system resources securely.
3. Kernel Execution: The kernel receives the system call request, identifies the specific service being requested, and executes the corresponding kernel function. This function performs the necessary operations, such as reading from a file, allocating memory, or sending data over the network.
4. Returning Results: Once the kernel completes the requested operation, it prepares the result (if any) and initiates a switch back to user mode.
5. Completion: The user-space application resumes execution, now with the results of the system call (e.g., data read from a file, confirmation of a successful operation).

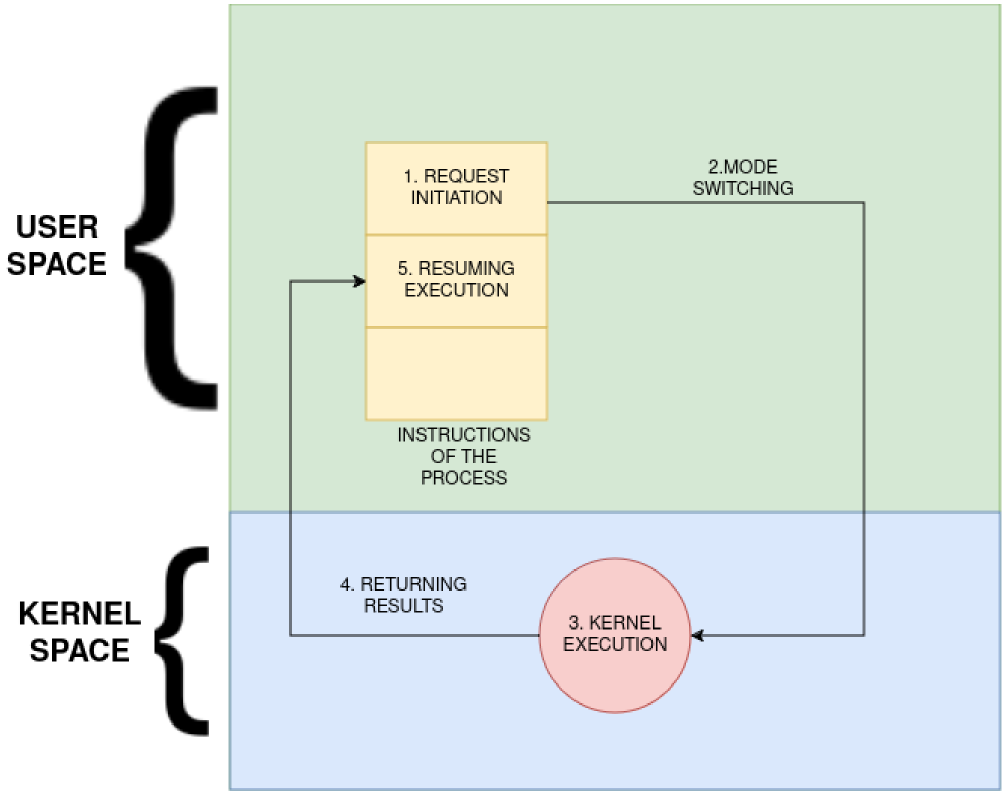

Figure 3: Kernel and User space

System calls are essential for maintaining system security and stability, as they control how user applications interact with hardware and critical system resources. By using system calls, operating systems ensure that all resource access requests are mediated, logged, and controlled, preventing unauthorized actions and maintaining the integrity of the operating system.

Monolithic operating systems

- Overview: A type of OS architecture where all OS services, like file management, device drivers, and networking, run in a single large block of code within the kernel.
- Characteristics: High performance due to minimal overhead; complex and difficult to maintain or debug because of its large, integrated codebase.

Layered operating systems

- Overview: An OS design where the operating system is divided into a hierarchy of layers, each built on top of the lower one.

- Characteristics: Each layer provides services to the layer above and relies on the layer below. This enhances modularity, making the operating system easier to develop and maintain, but can introduce performance overhead due to the multiple layers of abstraction.

Microkernels

- Overview: A minimalist OS architecture where the kernel only includes the most essential services, such as basic memory management, process scheduling, and inter-process communication.
- Characteristics: Other services (e.g., device drivers, file systems) run in user space. This design increases operating system reliability and security by isolating services, though it can suffer from performance overhead due to the frequent context switching.

Client-Server Model

- Overview: An OS structure based on the microkernel concept where services are separated into independent server processes that communicate with client processes.
- Characteristics: Promotes modularity and scalability. Each server can be developed, updated, and maintained independently, enhancing the operating system's flexibility and security.

Hypervisor

- Overview: An OS structure that allows multiple operating systems to run concurrently on a single physical machine by abstracting hardware resources into virtual machines.
- Characteristics: Provides strong isolation between different OS instances, supports efficient resource utilization, and facilitates testing and development by allowing multiple environments to coexist on the same hardware.

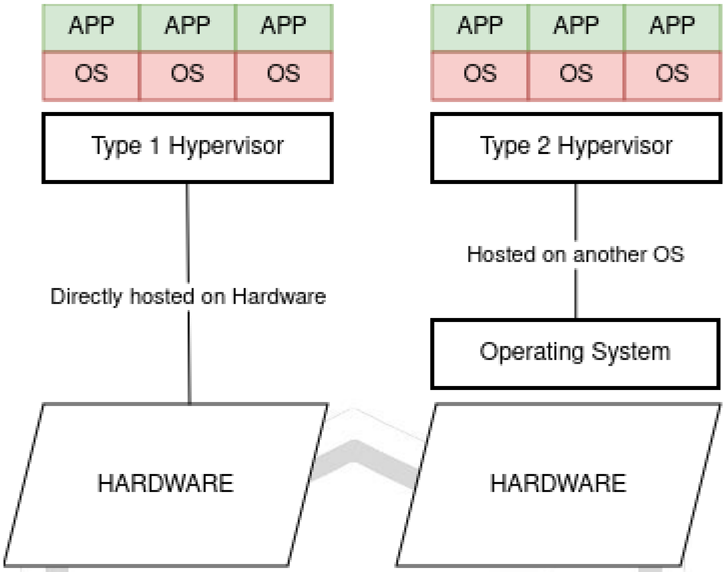

Figure 4: Types of Hypervisors

Exokernels and Uni-kernels

- Overview:
  - Exokernels: OS architecture that minimizes the kernel, providing applications with direct access to hardware resources.
  - Uni-kernels: Specialized OS images designed for a single application, containing only the necessary functionality for that application.
- Characteristics:
  - Exokernels: Maximize performance and flexibility by eliminating unnecessary abstractions, giving applications direct control over hardware.
  - Uni-kernels: Extremely efficient and secure due to their small size and tailored functionality, ideal for cloud and embedded environments where resource constraints and performance are critical.

Operating system (OS) security is a critical aspect of computing that aims to protect the system from unauthorized access, misuse, and threats, ensuring the confidentiality, integrity, and availability of data and resources. Key focus areas include authentication and access control, which verify user identities and manage permissions to restrict access to sensitive resources. Data encryption ensures that data stored or transmitted by the OS remains secure and unreadable by unauthorized parties. Operating system and network security involve protecting the OS from malware, viruses, and network-based attacks through firewalls, intrusion detection systems, and regular security updates. Vulnerability management includes identifying, assessing, and mitigating security flaws to prevent exploitation.

Additionally, audit and compliance mechanisms track system activity to detect suspicious behaviour and ensure adherence to security policies and regulations. Collectively, these focus areas help safeguard the system and the data it handles from a wide range of security threats.

The security requirements of Operating System are covered in Chapter-2 of this document.

Chapter-2 Security Requirements

Section 1: Access & Authorization

2.1.1 Role based access control policy

Requirement:

The operating system shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that determines how users interact with domains and resources. The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e., the specific operation command or command group (e.g. View, Modify, Execute). The operating system shall support RBAC with a minimum of 3 user roles, in particular, for privilege management for system management and maintenance, including authorization of the operation for configuration data and software.

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.2]

2.1.2 User Authentication

Requirement:

The various user and machine accounts on an operating system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, enables unambiguous authentication and identification of the authorized user. Authentication attributes include

- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker. For local access and machine accounts, at least one authentication attribute shall be supported.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.1]

2.1.3 Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform. Authorizations to an operating system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g. configuration and logging files). Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications shall not be executed with administrator or system rights.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.4 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the operating system. The operating system shall support the assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or an operating system. Operating system shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.2]

2.1.5 DAC Permissions

Requirement:

Discretionary Access Control (DAC) permissions on system files must be configured. DAC provides security measures by allowing resource owners to grant or restrict access to objects based on user identity and permissions thereby enhancing security.

[References: CIS Distribution Independent Linux v2.0.0 - 07-16-2019 section 6]

2.1.6 MAC Controls

Requirement:

There must be MAC (Mandatory Access Control) controls such as SElinux or AppArmor implemented at OS level which provides access control for the processes. MAC enforces strict security policies by controlling access to objects (such as files, data, or resources) based on predefined rules, thereby preventing any unauthorized access and enhancing overall security.

[References: ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.3]

Section 2: Authentication Attribute Management

2.2.1 Policy regarding consecutive failed login attempts

Requirement:

a. The maximum permissible number of consecutive failed user account login attempts shall be configurable by the operator. The definition of the default value set at manufacturing time for the maximum number of failed user account login attempts shall be less than or equal to 8, typically 5. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user, there shall be a block delay in allowing the user to attempt login again. This block delay and the capability to set the period of the block delay, e.g., double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure shall be configurable by the operator. The default value set at manufacturing time for this delay shall be greater than or equal to 5 sec.
b. If supported, infinite (permanent) locking of an account that has exceeded the maximum permissible number of consecutive failed user account login attempts shall also be possible via configuration, with the exception of administrative accounts, which shall get only temporarily locked.

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.5]

2.2.2 Suspend accounts on non-use

Requirement:

It shall be possible for the operating system to automatically suspend an account after 'X' days without a valid login. Note: X may be specified by OEM.

[Reference: CIS Password Policy Guide]

2.2.3 Protection against brute force and dictionary attacks

Requirement:

A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in the operating system. Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts. Various measures or a combination of the following measures can be taken to prevent this:

a. Using the timer delay (this delay could be the same or increased depending on the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
b. Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.
c. Using an authentication attribute blacklist to prevent vulnerable passwords.
d. Using CAPTCHA to prevent automated attempts.
e. Using Biometric Authentication
f. Using Provably Secure Token Based Authentication (For Ex - FIDO 2).

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by the operating system. An exception to this requirement is machine accounts.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

a. The configuration setting shall be such that an operating system shall only accept passwords that comply with the following complexity criteria:
   i) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the operating system). It shall not be possible setting this absolute minimum length to a lower value by configuration.
   ii) Password shall mandatorily comprise all the following four categories of characters: - at least 1 uppercase character (A-Z) - at least 1 lowercase character (a-z) - at least 1 digit (0-9) - at least 1 special character (e.g. @;!$.)
b. The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.

c. When a user is changing a password or entering a new password, the operating system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used. Passwords shall not be stored in clear text in the operating system; passwords shall be salted and hashed. Additionally, pepper may be included to increase the complexity i.e. password hash is a function of password, salt and pepper.

[Reference: 1) TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3
2) IETF draft-ietf-kitten-password-storage-04-BCP]

2.2.5 Inactive session timeout

Requirement:

User interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period. The operating system shall monitor inactive sessions of administrative login users and initiate session locking mechanisms based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID timeout must occur after this inactivity. Reauthentication of the user shall be repeated following any period of inactivity lasting 15 minutes or longer.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:

If a password is used as an authentication attribute, then the operating system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it shall be possible to implement this function on this operating system. Password change shall be enforced after initial login (After successful authentication). Operating system shall enforce password change based on password management policy. In particular, the OS shall enforce password expiry. OS shall support a configurable period for expiry of passwords. Previously used passwords shall not be allowed up to a certain number (Password History). The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its minimum value shall be 3.

This means that the operating system shall store at least the three previously set passwords. The maximum number of passwords that the OS 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. Above requirements shall be applicable for all passwords used. An exception to this requirement is machine accounts. The OS has an in-built mechanism to support this requirement. The minimum password age shall be set as one day i.e. recycling or flipping of passwords to immediate return to favourite password is not possible.

[Reference: 1) TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.2 2) CIS Password Policy Guide]

2.2.7 Protected Authentication feedback

Requirement:

The Authentication attribute 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 are replaced by a character such as "*".

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled or changed. Normally, authentication attributes such as password or cryptographic keys will be pre-configured from the producer, OEM or developer of an operating system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the operating system or the OEM provides instructions on how to manually change it.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:

The operating system shall have a function that allows a signed-in user to logout at any time. All processes under the logged-in user ID shall be terminated on logout. The operating system shall be able to continue to operate without interactive sessions. Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.1]

Section 3: Software Security

2.3.1 Secure Update

Requirement:

For software updates, the operating system shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only. To this end, the operating system must have a list of public keys or certificates of authorized software sources, and shall use the keys to verify that the software update is originated from only these sources.

Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

a. The system’s software package integrity shall be validated in the installation /upgrade stage.
b. The operating system shall support software package integrity validation via cryptographic means, e.g., digital signature, code signing certificate (valid and not time expired) using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only. To this end, the operating system must have a list of public keys or certificates of authorized software sources and shall use the keys to verify that the software update originated from only these sources.
c. Tampered software shall not be executed or installed if the integrity check fails.

d. A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in (ii) above.

Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:

a. OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).
b. Also, OEM shall submit the undertaking as below:
   i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the system software which includes OEM developed code, third party software and open-source code libraries used/embedded in the operating system.
   ii) System software shall be free from CWE top 25, OWASP top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plans.
   iii) The binaries for operating systems and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in [ii] above.

2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that the operating system is free from all known malware and backdoors as on the date of offer of operating system to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the operating system to the designated TSTL.

2.3.5 No Unused Software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the operating system shall not be present. Orphaned software components /packages shall not be present in the operating system. OEM shall provide a Software Bill of Materials (SBOM). A SBOM is a formal record containing the details and supply chain relationships of various open source and commercial software components, libraries and modules used in building software. In addition, OEM shall furnish an undertaking as "System does not contain Software that is not used in the functionality of system".

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:

The system shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. The system shall not support following services

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP - SNMPv1 and v2
- SSHv1 - TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD
- MOP

Any other protocols, services that are vulnerable are also to be permanently disabled. Full documentation of required protocols and services (communication matrix) of the system and their purpose needs to be provided by the OEM as a prerequisite for the test case.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Restricting OS Boot Source

Requirement:
The operating system can boot only from the memory devices intended for this purpose.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section- 4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:

The reliable time and date information shall be provided through NTP/PTP server. All elements/functions which require timestamps shall establish a secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" with NTP/PTP server. Audit logs shall be generated for all changes to time settings.

2.3.9 Self-Testing

Requirement:

A cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

Section 4: System Secure Execution Environment

2.4.1 No unsupported components

Requirement:

OEM to ensure that the operating system shall not contain software components that are no longer supported by them or their 3rd Parties including the open-source communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be given by the OEM.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.5]

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement:

The security event log shall be access controlled (file access rights) such that only privileged users have access to the log files.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

The operating system shall log all important security events with unique operating system reference details as given in the Table below. OS shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, protocol, service or program used for access, source and destination IP addresses & ports and the outcome (success or failure) of the event. Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event types (Mandatory or optional)	Description	Event data to be logged
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the operating system.	Username
		Source (IP address and ports) if remote access
		Outcome of event (Success or failure)
		Timestamp
		Username,
		Timestamp,

Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Length of session
		Outcome of event (Success or failure)
		Source (IP address &port) if remote access
Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username,
		Administered account,
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Resource Usage (Mandatory)	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 operating system.
		Outcome of event (Threshold Exceeded)
		Timestamp
Configuration change (Mandatory)	Changes to configuration of the operating system.	Change made
		Timestamp
		Outcome of event (Success or failure)

		Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the operating system that forces a reboot or shutdown OR where the operating system has crashed.	Action performed (boot, reboot, shutdown, etc.)
		Username (for intentional actions)
		Outcome of event (Success or failure)
		Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the operating system (e.g. shutdown)	Interface name and type
		Status (shutdown, down missing link, etc.)
		Outcome of event (Success or failure)
		Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	Administrator username,
		Administered account,
		Activity performed (group added or removed)
		Outcome of event (Success or failure)
		Timestamp.
Resetting Passwords	Resetting of user account	Administrator username
		Administered account
		Activity performed (configure, delete, enable and disable)

(Optional)	passwords by the Administrator	Outcome of event (Success or failure)
		Timestamp
Services (Optional)	Starting and stopping of services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	Attempt to initiate manual update, initiation of update, completion of update	User identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	Old value of time Subject identity
		New value of time
		Timestamp

		origin of attempt to change time (e.g. IP address)
		Outcome of event (Success or failure)
		User identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session.	User identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorized remote administrators (Optional)	Initiation, Termination and Failure of Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
		Timestamp
		Type of event (audit data deletion, audit data modification)

Audit data changes (Mandatory)	Changes to audit data including deletion of audit data	Outcome of event (Success or failure)
		Subject identity
		User identity
		origin of attempt to change time (e.g. IP address)
		Details of data deleted or modified
User Login and Logoff (Mandatory)	All use of Identification and authentication mechanisms.	User identity
		Origin of attempt (IP address and port)
		Outcome of event (Success or failure)
		Timestamp

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Logging access to personal data

Requirement:

In some cases, access to personal data in a clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes, such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of user. In such cases, the revealed personal information may not expose the user to any kind of privacy violation.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.5]

2.5.4 Security audit log

Requirement:

The security audit log must not contain

1. Authentication credentials, even if encrypted (e.g. password)
2. Access Tokens-To be masked when outputting
3. Proprietary or sensitive personal information.

[Reference: GSMA NG 133 Cloud Infrastructure Reference Architecture Ver 2.0 6.3.7.3]

2.5.5 Audit Logs

Requirement:

1. All security logging mechanisms must be active from OS initialization
2. Logs must be time synchronized.
3. Security audit logs must be accessible only by authorized users.
4. The following system events must be logged (apart from those listed in 2.5.2)
    a. Successful and unsuccessful changes to privilege level
    b. Successful and unsuccessful security policy changes
    c. Starting and stopping of security logging
    d. Starting and stopping of processes including attempts to start unauthorized processes.
    e. All command line activity performed by innate OS programs known to otherwise leave no evidence upon command completion.

[Reference: GSMA NG 133 Cloud Infrastructure Reference Architecture ver 2.0 6.3.7.1 & 6.3.7.2]

Section 6: Data Protection

2.6.1 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the system (in the form of software, hardware or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards. Till further instructions, this clause will be considered ‘complied’ by submission of an undertaking by the OEM in specified format along with self-certified test reports. An undertaking is to be submitted by the OEM mentioning that “Cryptographic module embedded inside the system (in the form of software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards".

2.6.2 Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithms implemented inside the Crypto module of the system shall be in compliance with the respective FIPS standards (for the specific crypto algorithm). Till further instructions, this clause will be considered 'compiled' by submission of an undertaking by the OEM in specified format along with self-certified test reports. An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithm implemented inside the Crypto module of the system is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the system)".

2.6.3 Protecting data and information in storage

Requirement:

a. For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of operating system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.
b. In addition, the following rules apply for:
    i) Operating systems that need access to identification and authentication data in the clear/readable form e.g. in order to perform an activity/operation shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
    ii) Operating systems that do not need access to sensitive data in the clear shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
    iii) Stored files in the system: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

Section 7: Network Services

2.7.1 Traffic Filtering – Network Level Requirement

Requirement:

The operating system shall provide a mechanism to filter incoming IP packets on any IP interface. In particular, the operating system shall provide a mechanism:

a. To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.

b. To allow specific actions to be taken when a filter rule matches. In particular at least the following actions shall be supported:

   i) Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.

   ii) Accept: the matching message is accepted.

   iii) Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

c. To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.

d. To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.

e. To reset the accounting.

f. The operating system shall provide a mechanism to disable/enable each defined rule.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.1]

Section 8: Attack Prevention Mechanisms

2.8.1 Manipulated packets that are presented to an operating system shall not lead to an impairment of availability.

Requirement:

The operating system shall not be affected in its availability or robustness by incoming packets from outside sources that are manipulated or differing from the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of the operating system. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets. Examples of such packets are:

a. Mass-produced TCP packets with a set SYN flag to produce half-open TCP connections (SYN flooding attack).
b. Packets with the same IP sender address and IP recipient address (Land attack).
c. Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
d. Fragmented IP packets with overlapping offset fields (Teardrop attack).
e. ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IPv4 packets (Ping-of-death attack).
f. Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the operating system/DUT in fulfilment of this clause.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.6.2.2]

Section 9: Vulnerability Testing Requirements

2.9.1. Vulnerability Scanning

Requirement:

The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide a remediation plan.

Sl. No.	CVSS Score	Severity	Remediation
1	9.0-10.0	Critical	To be patched immediately
2	7.0-8.9	High	To be Patched within a month
3	4.0-6.9	Medium	To be patched within three months
4	0.1-3.9	Low	To be patched within a year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Reference 1: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.3
Reference 2: GSMA NG 133 Cloud Infrastructure Reference Architecture]

Section 10: Core operating system

2.10.1. Growing Content Handling

Requirement:

a. Growing or dynamic content shall not influence operating system functions.
b. A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop the operating system from operating properly. Therefore, counter measures shall be taken to ensure that this scenario is avoided.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2. Handling of IP options and extensions

Requirement:

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.2.4.1.1.3]

2.10.3. Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the operating system. The system shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to

0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request ")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet too Big	Permitted	N/A
N/A	135	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

The system shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e., do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. 4.2.4.1.1.2.]

2.10.4. Authenticated Privilege Escalation only

Requirement:

The OS shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.2.1]

2.10.5. System account identification

Requirement:

Each system account SHALL have a unique identification with appropriate non-repudiation controls.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.2.2]

2.10.6. OS Hardening - Minimized kernel network functions

Requirement:

Kernel-based network functions not being used shall be deactivated. In particular, the following ones shall be disabled by default:

a. IP Packet Forwarding between different interfaces
b. Directed broadcast
c. IPv4 Multicast handling
d. Gratuitous ARP messages
e. Proxy ARP

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.2]

2.10.7. No automatic launch of removable media

Requirement:

The OS shall not automatically launch any application when a removable media device is connected.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.3]

2.10.8. External File System mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), restrictions shall be set properly in the operating system in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems. Restrictions shall apply to normal users against mount / use of removable media devices (e.g. USB drive, CD ROM etc.) for data transfer.

[Reference– TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.6]

2.10.9. File System Authorization privileges

Requirement:

The OS shall be designed to ensure that only users that are authorized to modify files, data, directories, or file systems have the necessary privileges to do so.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.2.7]

2.10.10. SYN Flood Prevention

Requirement:

The OS shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.4]

Section 11: Kernel Security Requirements

2.11.1. ASLR (Address space layout randomization) & KASLR (Kernel Address space layout randomization)

Requirement:

ASLR (Address space layout randomization) & KASLR (Kernel Address space layout randomization) must be enabled.

ASLR is an exploit mitigation technique which randomly arranges the address space of key data areas of a process. KASLR is an exploit mitigation technique that mitigates memory access vulnerabilities by randomizing the base address value of the kernel.

[Reference: CIS Distribution Independent Linux Benchmark v2.0.0 - 07-16-2019 Section J1.5.3]

2.11.2. IMA (Integrity Measurement Architecture)

Requirement:

IMA must be enabled. It shall measure unauthorized access to the files and kernel modules.

[Reference: RedHat "How to use the Linux kernel's Integrity Measurement Architecture" October 22,2020]

2.11.3. Kernel Memory Sanitizers

Requirement:

Kernel Memory Sanitizers shall be in place to detect uninitialized memory accesses. For example, KMSAN is used to detect uninitialized memory accesses to Linux kernel. KMSAN works by instrumenting the kernel code at compile time and checking for accesses to uninitialized memory at run time.

[Reference: The Linux Kernel ver. next-20240617 "Kernel Memory Sanitizer (KMSAN)"8]

2.11.4. Kernel Memory Leak Detector

Requirement:

The kernel shall be configured and booted with Kernel Memory Leak Detector enabled. The operating system shall have procedures in place to regularly monitor for potential memory leaks.

[Reference: The Linux Kernel 6.10.0-rc4 "Kernel Memory Leak Detector"]

2.11.5. Kernel Page Table isolation

Requirement:

Kernel Page Table isolation (KPTI) must be enabled in the Operating System to protect against vulnerabilities like meltdown.
KPTI is a critical security feature that protects against vulnerabilities like Meltdown (Reading Kernel Memory from User Space) by isolating user space and kernel space memory through separate page tables.

[Reference: The Linux Kernel next-20230330 “Page Table Isolation (PTI)”]

2.11.6. Shadow Stack

Requirement:

Shadow stack protection must be enabled. Stack shall be split into two distinct areas storing precious variables and user variables in non-contiguous memory areas. Shadow stack protection shall make it more difficult to smash one of the stacks from the other.

2.11.7. Encrypted Storage

Requirement:

All the disks including the swap partition must be encrypted. The passphrase or keys used to encrypt these disks must be stored in a secure location (e.g. TPM, HSM).

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T14]

2.11.8. Custom kernel module signing

Requirement:

Custom kernel modules must be signed and verified when loaded. When custom modules are developed, they must be signed, and, upon loading, these modules must be verified against the key to ensure their authenticity and integrity.

2.11.9. Stack Smash Protection

Requirement:

To enhance code security in production environments:

1. Stack Canaries shall be implemented during compilation or interpretation (e.g., using the -fstack-protector flag in GCC Compiler).
2. Additionally, Hardware-based Data Execution Prevention (DEP) shall be enabled.

If Hardware-based DEP (e.g., NX Bit on modern processors) is unavailable, OEMs must provide a signed document confirming its absence, necessitating the implementation of Software-based DEP. Activating this feature mitigates buffer overflow vulnerabilities and must be enabled whenever feasible.

[Reference: CIS Distribution Independent Linux v2.0.0 - 07-16-2019 section 1.5.2]

Section 12: Other Security requirements

2.12.1. No Root Password Recovery

Requirement:

No provision shall exist for OS's root password recovery.

2.12.2. Secure System Software Revocation

Requirement:

Once the system software image is legally updated/upgraded with a new software image, it shall not be possible to roll back to a previous software image. In case roll back is essential, it shall be done only by the administrator with appropriate non- repudiation controls. OS shall support a well-established control mechanism for rolling back to previous software images.

2.12.3. Software Integrity Check –Installation

Requirement:

Operating system, shall validate the software package integrity before the installation stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only. Tampered software shall not be executed or installed if integrity check fails.

2.12.4. Software Integrity Check – Boot

Requirement:

The operating system shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

2.12.5. No Default Profile

Requirement:

Predefined or default user accounts (other than Admin/Root) in the operating system shall be deleted or disabled.

2.12.6. No unused File System

Requirement:

File systems which are not needed for operation or functionality of the operating system shall not be present. OEM shall provide the list of file systems that are necessary for operating system's operation. In addition, OEM shall furnish an undertaking as "operating system does not contain file system that is not used in the functionality of operating system"

[Reference: CIS Distribution Independent Linux v2.0.0 - 07-16-2019 section 1.1.1]

2.12.7. Bootloader Configuration

Requirement:

a. Bootloader must be configured such that read and write permission is only given to root users.
b. Ensure Bootloader password is set.

[Reference: CIS Distribution Independent Linux v2.0.0 - 07-16-2019 section 1.4]

2.12.8. File System partitions and mount options configuration

Requirement:

File system partitions and mount options shall be configured in the operating system. Creating separate partitions prevent users from filling up the root file system and mounting with options nodev, nosuid, noexec prevent device file creation, setuid program execution, and binary execution that enhances the operating system security.

[Reference: CIS Distribution Independent Linux v2.0.0 - 07-16-2019 section 1.1.2-1.1.21]

2.12.9. Resource Requests and Limits

Requirement:

It shall be possible to apply different object level resource requests and limits via CGroups so as to prevent rogue workloads exhausting the node and cluster level resources.

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

2.12.10. Runtime Security

Requirement:

Syscalls shall be restricted to an allow-list to decrease the application's attack surface. For example, seccomp-bpf can be used. Incase SecComp is used to restrict syscalls, strict mode shall only be used for scenarios requiring the absolute minimum of system calls (to be specified by OEM).

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part II: Securely Isolate Network Resources,2021]

2.12.11. Namespaces

Requirement:

OS must provide a mechanism to apply different object level isolation via namespaces so as to prevent rogue workloads from accessing resources of another workload.

2.12.12. Pre-Linking Programs

Requirement:

There are many programs that modifies Executable and Linkable Format (ELF) shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases. These programs shall not be present in the operating system. OEM shall furnish an undertaking for the above.

[Reference: CIS Distribution Independent Linux v2.0.0 - 07-16-2019 section 1.5.4]

2.12.13. Core Dump

Requirement:

OS shall provide a mechanism to set a hard limit on core dumps. If core dumps are required in that particular OS by the OEM, the OEM will have to specify to the tester to make an exception.

[Reference: CIS Distribution Independent Linux v2.0.0 - 07-16-2019 section 1.5.1]

Annexure-I

Definitions

1. **ABAC:** Attribute-based access control (ABAC), also known as policy-based access control for IAM, defines an access control paradigm whereby a subject's authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment attributes.
2. **Address Space:** An address space refers to the set of memory locations available to a process, encompassing all the addresses it can access for its code, data, and stack during execution.
3. **Anti-Spoofing:** Anti Spoofing is a technique for identifying and dropping packets that have a false source address Application Programming Interface: This interface can be thought of as a contract of service between two applications
4. **Atomic deployable unit:** An instance of an atomic deployable unit is represented by a single VM for hypervisor-based virtualization or represented by one or a set of OS containers for CIS (Container Infrastructure Service) based virtualization.
5. **Availability:** The network availability is the average percentage of time during which the network is performing its intended function.
6. **CGroups:** It is short for Control Groups. It is a Linux kernel feature that limits, accounts for, and isolates the resource usage (CPU, memory, disk I/O, network, etc.) of a collection of processes.
7. **Chain of trust:** It is used to infer trust in the measurement data of the software component that represents the last link of the chain
8. **Confidentiality:** The state of keeping or being kept secret or private.
9. **Confidential system internal data:** that contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).
10. **Core Dump:** A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The operating system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.
11. **Files:** Files are structured units of data stored on a computer, typically on a disk, that are used to organize and manage information.
12. **Firewall:** A firewall is a network security device that monitors traffic to or from the network.

13. **Host operating system:** collection of hardware, software and firmware making up the operating system which executes workloads
14. **Hypervisor:** A software which acts as a bridge in between the Virtual Machines and the Host machine. It converts all the operations from the Virtual Machines so that they will be executable on the Host Machine CPU. It is informally called an operating system for operating systems.
15. **Kernel:** The kernel serves as the central component of an operating system, responsible for handling essential tasks such as managing hardware resources, facilitating communication between hardware and software, and ensuring the smooth execution of processes. If you strip away all the UI and frontend of all operating systems, what is left is the kernel.
16. **Least Trusted Domain (LTD):** The Less Trusted Domain (LTD) contains resources that can be managed without the risk of compromising sensitive information, since these functionalities are offloaded to the MTD. More Trusted Domain (MTD) contains resources (network, storage, processing) where sensitive functions can be offloaded.
17. **Memory:** The memory is the part of a computer system responsible for holding data and program instructions that the CPU needs to execute tasks.
18. **Namespace:** In OS, namespaces provide a mechanism for isolating groups of resources within a single cluster.
19. **Operating System:** A software program that manages the execution of application programs and serves as an intermediary between the computer user and the computer hardware.
20. **Personal data:** "personal data" means any data about an individual who is identifiable by or in relation to such data;
21. **Platform:** A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.
22. **Post-incident analysis:** post-incident analysis is the checking of various logged measurements to establish details of the attack, i.e. the mode and method of attack, the time of the attack, the identities or locations of attackers.
23. **Process:** A process is a dynamic execution state of a program, including the program's instructions, its current execution status, and the resources it uses, such as memory and I/O devices.
24. **Sensitive Data:** data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, or IP addresses of the operating system, as well as file
25. **Stack Buffer:** A stack buffer is a designated area of the process's stack memory where temporary data is stored. This includes function parameters, return addresses, and local variables essential for the execution of functions. The stack buffer plays a

crucial role in maintaining the process's execution state and facilitating smooth function call management. It is also one of the vulnerable areas of the process as the return address is manipulated for various buffer overflow attacks.

26. **Syscall:** The system call is the fundamental interface between an application and the Linux kernel.
27. **Virtual Machine (VM):** virtualized computation environment that behaves very much like a physical computer/server; A virtual machine (VM) is an isolated computing environment created by abstracting resources from a physical machine
28. **VM Image:** A Virtual Machine Image is a fully configured Virtual Machine used to create a VM for deployment.

Annexure-II

Acronyms

ARP	-	Address Resolution Protocol
CIS	-	Center for Internet Security
CLI	-	Command Line Interface
CNCF	-	Cloud Native Computing Foundation
CPU	-	Central Processing Unit
DAC	-	Discretionary Access Control
DM-verity	-	Device-Mapper-verity
ELF	-	Executable and Linkable Format
GUI	-	Graphical User Interface
ICMP	-	Internet Control Message Protocol
IDE	-	Integrated Development Environment
IE	-	Information Element
IMA	-	Integrity Measurement Architecture
IP	-	Internet Protocol
ISO-OSI	-	International organization of Standardization – Open system Interconnection
KAISER	-	Kernel Address Isolation to have Side channels Efficiently Removed
KMSAN	-	Kernel Memory Sanitizers
KPTI	-	Kernel Page Table Isolation
MAC	-	Media access control
OEM	-	Original equipment manufacturer
OS	-	Operating System
RAM	-	Random Access Memory
TEC	-	Telecommunication Engineering Centre
UE	-	User Equipment
VM	-	Virtual Machine

Annexure-III

List of Undertakings

List of Undertakings to be furnished by the OEM for Operating System Security testing submissions.

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and backdoor check (against test case 2.3.4)
3. No unused software (against test case 2.3.5)
4. No unsupported Components (against test case 2.4.1)
5. Cryptographic module Security Assurance (against test case 2.6.1)
6. Cryptographic Algorithms Implementation Security Assurance (against test case 2.6.2)
7. No unused File System (against test case 2.12.6)
8. Pre-Linking Programs (against test case 2.12.14)

Annexure-IV

References

1. CIS Distribution Independent Linux Benchmark v2.0.0 - 07-16-2019
2. CIS Ubuntu Linux 22.04 LTS Benchmark
3. CIS Password Policy Guide
4. CNCF Cloud Native Security Whitepaper Ver 2.0
5. ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.3
6. UCD_Linux_Security_Checklist
7. IETF draft-ietf-kitten-password-storage-04-BCP
8. Mastering Linux Security and Hardening Third Edition - Donald A. Tevault
9. Modern Operating Systems - Andrew S. Tanenbaum, Herbert Bos
10. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part II: Securely Isolate Network Resources,2021
11. GSMA NG 133 Cloud Infrastructure Reference Architecture Ver 2.0
12. RedHat "How to use the Linux kernel's Integrity Measurement Architecture" October 22, 2020
13. TEC 25848:2022
14. TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. "Catalogue of General Security Assurance Requirements".