GTI Security Test Guide for eMBB Device

GTI Security Test Guide for eMBB Device

Version	V0.1
Deliverable Type	□Procedural Document √Working Document
Confidential Level	□Open to GTI Operator Members □Open to GTI Partners √Open to Public
Program Name	5G ENS
Project Name	Security
Source members	CMCC
Support members	
Editor	Songquan Shi(CMCC) ,Qiguang Fan(CMCC), Le Yu(CMCC), Kai Yang(CMCC),Huaxi Peng(CMCC)
Last Edit Date	12-06-2021
Approval Date	12-06-2021

Document History

Date	Meeting #	Version #	Revision Contents
2021-12-8		0.1	

Table of Contents

1 Executive Summary

The specifications of 5G NR in Standalone operation are due for completion in June 2018, which will provide a complete set of specifications for the 5G Core Network that goes beyond Non-Standalone. The'full' 5G System includes:

- eMBB (enhanced Mobile Broadband)
- URLLC (Ultra Reliable Low Latency Communications)
- mMTC (massive Machine Type Communications)

Providing significant benefits to consumers, enhanced mobile broadband (eMBB) will be an extension to existing 4G network and will be amongst the first wave of the 5G services. Changes in device function and structure will also bring some new security risks. In order to make the terminal more secure to deal with new hardware security and new data security, the device needs some security functions to ensure the normal operation of its own services and functions.

The purpose of this document is to enable the suppliers of eMBB devices to assess the conformance of their devices to the GTI Security test Guide for 5g eMBB device . Completing a GTI Security Assessment will allow an entity to demonstrate the security measures they have taken to protect their products .

This document is the test for "Security Technical Implementation Guide for 5G eMBB devices", The purpose of this document is to enable emBB device suppliers to evaluate whether their device has basic security capabilities.

2 Abbreviations

Abbreviation	Explanation
eMBB	enhanced Mobile Broadband
OTA	Over-the-Air Technology
ADB	Android Debug Bridge
SSH	Secure Shell
USB	Universal Serial Bus
MAC	Media Access Control
APP	Application
DHCP	Dynamic Host Configuration Protocol
SSID	Service Set Identifier
WPA	Wi-Fi Protected Access
EAP	Extensible Authentication Protocol

3 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[1] GTI Security Technical Implementation Guide for 5G eMBB devices

4 Test Environment

Test Environment is shown in the Figure1, including eMBB device, service platform , test computer and other auxiliary tools (such as UART tool etc.). eMBB device and service platform compose the environment to be test , the computer installed with Various Safety Detection Software Tools work in with other auxiliary tools to do the check.

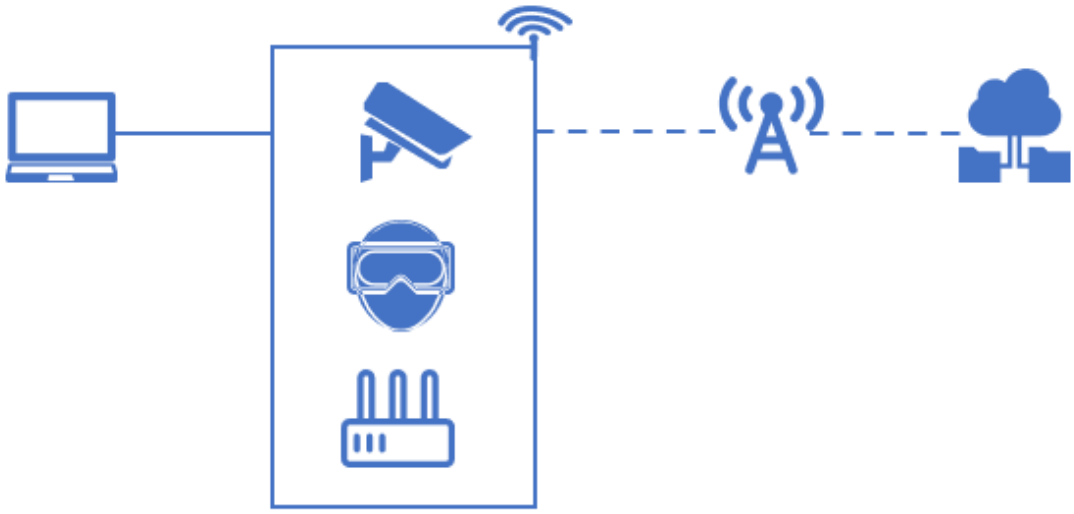

Figure 1 A simple Diagram of Test Environment

5 Hardware Security Test

Task code	Description	Test procedure
Hardware security Interface-01	The identity Authentication is needed for devices with console to prevent direct login.	1. Restore device to factory settings; 2. If console is available,try to login through the console with debugging tools to check whether user name and password are needed.
Task result	Login with debug port requires user name and password: Yes☐ Part☐ No ☐ N/A☐	
Hardware security Interface-02	When the wired peripheral interface establishes the data connection, it should give the user the corresponding state change prompt,	1. Restore device to factory settings; 2. Let device run for a while 3. check the indicator light status
Task result	The indicator light shows the data transmission status, when data transmission Yes☐ Part☐ No ☐ N/A☐	
Hardware security chip-01	Support the trusted execution environment, provide the isolation of security area and non-security area (optional).	Prerequisite:The hardware design documentation is needed. Check whether the chip supports TEE
Task result	The chip supports TEE Yes☐ Part☐ No ☐ N/A☐	

6 System Security Test

Task code	Description	Test procedure
System security System upgrade-01	At least have the ability to update automatically or manually.	Prerequisite:The system design documentation is needed. 1. Check whether the automatically update functioin is available . 2. Check whether the manually update functioin is available .
Task result	The manually update function& automatically update function is available Yes☐ Part☐ No ☐ N/A☐	
System security System upgrade-02	The firmware source provides firmware verification data to ensure that the system can confirm the integrity of the firmware before upgrading.	Prerequisite:The Official Upgrade package is needed. 1. Modify the official upgrade package. 2. Upgrade the device through the modified upgrade package. 3. Check whether the upgrade is successful.
Task result	The upgrade is not successful Yes☐ Part☐ No ☐ N/A☐	
System security System Privilege Restrictions-01	The multi-user system design should conform to the Principle Of Least Privilege and the users should be given the minimum privilege required to perform the task , all unauthorized permissions should be prohibited .	Prerequisite:The system design documentation is needed. 1. Check the system design documentation to determine whether multi-user is available . 2. If multi-user is available , login as an normal user and try to modify the system configuration file .
Task result	The system configuration file can not be modified when login as normal user . Yes☐ Part☐ No ☐ N/A☐	

System security Configuration-01	The important partition（boot,system）should be configured as read-only mode .	Prerequisite:The system design documentation is needed. 1. Check the system design documentation to determine the path of important partition . 2. try to modify the file in important partition .
Task result	The file in important partition can not be modified. Yes☐ Part☐ No ☐ N/A☐	
System security Configuration-02	For devices with debug function, the privilege of debug process in the operating system permissions should be severely restricted,to prevent the abuse of privilege.	Prerequisite:The system design documentation is needed. 1. Check the system design documentation to determine the privilege of debug port . 2. Login through the debug port with debugging tools , try to modify the file that don't permit to modify.
Task result	The file can not be modified . Yes☐ Part☐ No ☐ N/A☐	
System security Configuration-04	System services should follow the principle of least privilege.In addition to the necessary service port, the number of open ports should be minimized	Prerequisite:The system design documentation is needed. 1. Check the system design documentation to determine the necessary service port . 2. Login the system and check whether the unnecessary service port is open.
Task result	The unnecessary service port is not open . Yes☐ Part☐ No ☐ N/A☐	
System security Configuration-05	For systems with configurable services, the ability to modify the default configuration is necessary.	1. Restore device to factory settings; 2. Try to modify the default

	The system security functions should include the but not limited to the following list: modifying default identity, changing authentication information,configuring service on and off by default, restricting and monitoring application access, background data refresh.	system configuration .
Task result	The default system configuration can be modified . Yes☐ Part☐ No ☐ N/A☐	
System security Encryption and Authentication-01	The system has the ability of unified authentication and security context management for heterogeneous access to improve the efficiency of security context switching for heterogeneous access.	Prerequisite:The system design documentation is needed. 1. Check whether support EAP(Extensible Authentication Protocol).
Task result	The system support EAP Yes☐ Part☐ No ☐ N/A☐	

7 Application Security Test

Task code	Description	Test procedure
Application Security Built-in application-01	The use of hard-coded password should be avoided.	1. Extracting file system from the firmware . 2. Check all files in the file system to determine whether hard-coded password exist .
Task result	The hard-coded password is not exist . Yes☐ Part☐ No ☐ N/A☐	

8 Data Security Test

Task code	Description	Test procedure
Data Security Data Storage-01	The function of securely encrypt sensitive information is needed, explicitly record sensitive information in logs and configuration files should be forbidden.	Prerequisite:The path of system log and important files(Including but not limited to password file , The application context file) is needed. 1. Use the device for a period of time normally . 2. Check the important files to determine whether unencrypted sensitive information exist .
Task result	Unencrypted sensitive information is not exist . Yes☐ Part☐ No ☐ N/A☐	
Data Security Log-01	For devices that are remotely managed through Web, managing and configuring device profile should be forbidden without authentication, and the authentication process must be logged in detail.The content of the record should include user account,login status, login time, and user's IP address.	Prerequisite:The path of system log is needed. 1. Use the device for a period of time normally . 2. Check the system log to determine whether login detail exist .
Task result	The content of the record includes user account,login status, login time, and user's IP address. Yes☐ Part☐ No ☐ N/A☐	
Data Security Log-02	The ability to record the operation on the device is needed, which including but not limited to the followings: operating account, operating time, operating content and operating results.	Prerequisite:The path of system log is needed. 1. Use the device for a period of time normally . 2. Check the system log to determine whether Usage detail exist .

Task result	The content of the record includes operating account, operating time, operating content and operating results. Yes☐ Part☐ No ☐ N/A☐	
Data Security Log-03	Unexpected shut down, restart,file system collapse of device should be logged automatically.	Prerequisite:The path of system log is needed. 1. Use the device for a period of time normally , and cut the power . 2. Check the system log to determine whether abnormal information exist .
Task result	The abnormal information is recorded in the log . Yes☐ Part☐ No ☐ N/A☐	

Appendix

Example of typical device test results

Device type	**5g HD camera**
Hardware architecture	**ARM**
Firmware version	******-RD50X40C**
Kernel version	**Linux Kernel 3.10.10**
Test time	**2021-09-29**

Hardware Security Test

Task code	Test procedure
Hardware security Interface-01	1、The UART interface is exposed 2、Login from the interface does not require password authentication
	Login with debug port requires user name and password: Yes☐ Part☐ No ☑ N/A☐
Hardware security Interface-02	There are indicators to indicate connection and data transmission status
	The indicator light shows the data transmission status, when data transmission Yes☑ Part☐ No ☐ N/A☐
Hardware security chip-01	The CPU is ARM architecture, Not using TrustZone
	The chip supports TEE Yes☐ Part☐ No ☑ N/A☐

System Security Test

Task code	Test procedure
System security System	Update options are available on the configuration page

upgrade-01	The manually update function& automatically update function is available Yes☑ Part☐ No ☐ N/A☐
System security System upgrade-02	1.Modify the official upgrade package. 2.Updater failed
	The upgrade is not successful Yes☑ Part☐ No ☐ N/A☐
System security Configuration-01	Run “mount” command, all partition is RW
	The file in important partition can not be modified. Yes☐ Part☐ No ☑ N/A☐
System security Configuration-04	Run “netstat” command, unnecessary service port is not open
	The unnecessary service port is not open. Yes☑ Part☐ No ☐ N/A☐
System security Encryption and Authentication-01	
	The system support EAP Yes☐ Part☐ No ☐ N/A☑

Application Security Test

Task code	Test procedure
Built-in application-01	1. Decompile the main services application. 2. There is unencrypted command, can open Telnet service from remote
	The hard-coded password is not exist . Yes☐ Part☐ No ☑ N/A☐

Data Security Test

Task code	Test procedure
Data Security Data Storage-01	1. Use the device for a period of time normally . 2. Login the device with debug port, enter the folder where system logs and important files are stored.

	3. The WIFI password is in plain text
Task result	Unencrypted sensitive information is not exist . Yes☐ Part☐ No ☑ N/A☐
Data Security Log-01	1. Use the device for a period of time normally . 2. Login the device with debug port, enter the folder where system logs and important files are stored. 3. Log files exist，Includes time, users, and so on
Task result	The content of the record includes user account,login status, login time, and user's IP address. Yes☑ Part☐ No ☐ N/A☐
Data Security Log-02	1. Use the device for a period of time normally . 2. Login the device with debug port, enter the folder where system logs and important files are stored. 3. None operating account, operating time being record.
Task result	The content of the record includes operating account, operating time, operating content and operating results. Yes☐ Part☐ No ☑ N/A☐
Data Security Log-03	1. Use the device for a period of time normally , and cut the power . 2. Login the device with debug port, enter the folder where system logs and important files are stored. 3. Check the system log to determine whether abnormal information exist .
Task result	The abnormal information is recorded in the log. Yes☐ Part☐ No ☑ N/A☐