GTI Security Technical Implementation Guide for 5G eMBB Devices

http://www.gtigroup.org

Security Technical Implementation Guide for 5G eMBB Devices

V 0.1

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	Qualcomm
Editor	Songquan Shi(CMCC), Qiguang Fan(CMCC), Jiangsheng Wang(Qualcomm), Le Yu(CMCC), Kai Yang(CMCC),Huaxi Peng(CMCC)
Last Edit Date	12-06-2021
Approval Date	12-06-2021

Document History

Date	Meeting #	Revision Contents	Old	New
2021/6/10				V0.1
2021/10/11				V0.2
2021-12-6				V0.3

Table of Contents

1. Introduction

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)

The year 2019 witnessed the first wave of standards-based 5G commercial launches. According to the Global mobile Suppliers' Association (GSA), 80 operators had launched 3GPP-compliant 5G commercial services across 42 countries (May 2020). Half of these had launched 5G fixed wireless access services, targeting areas lacking quality fixed broadband connectivity.

The emergence of 5G has potential to radically improve customer experience however poses new challenges to Network Operators, device manufacturers and telecom infrastructure.

The initial phase of 5G Non-Standalone deployments focuses on eMBB, which provides greater data-bandwidth complemented by moderate latency improvements on both 5G NR and 4G LTE. This will help to develop today's mobile broadband use cases such as emerging AR/VR media and applications, UltraHD or 360-degree streaming video and many more.

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. eMBB will transform user-experience, revolutionize the gaming industry with AR/VR cloud gaming and drive 4K video streaming as the new norm, However the full potential of 5G`s commercial benefits are yet to be discovered.

With the development of 5G, the devices will also be affected and changed:

- Devices will be put under new constraints and will require redesigning or retrofitted to ensure that they properly meet the demands of higher data-rates and power requirements.
- Devices are likely to become more complex, to satisfy consumers expectations for small or slim devices, reliability and miniaturisation of component technology and modualization will become a necessity.
- Increased transfer data rate mean higher device temperature - raising performance and security concerns - and will demand more efficient power distribution and battery life.
- eMBB will need to provide both higher capacity in congested areas and enhanced coverage for those on the move - Fixed wireless access (FWA) uses the mobile network to deliver internet to a household with a home gateway with integrated mobile technology then distributes the bandwidth as needed. 5G FWA can achieve up to 1Gbps bandwidth in some cases.

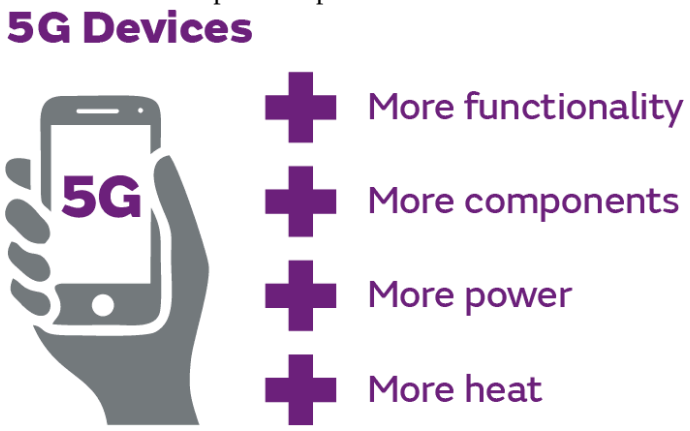

Fig. 1 changes on device

Changes in device function and structure will also bring some new security risks. In order to make device more secure to protect services, software, hardware, communication and data in 5G, the device needs some security functions to ensure the normal operation of its own services and functions.

2. Abbreviations

Abbreviations

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

3. Security advices for 5G eMBB devices

5.1. Hardware security advices

5.1.1. Interface

1. For devices with console, user name and password should be configured for authentication and authorization, and non-authenticated access is forbidden.
2. When the wireless peripheral interface establishes data connection, the device with display function shall be able to provide the user with the function of monitoring data transmission status, such as providing indicator light or display screen, to prevent illegal connection, illegal data access or illegal data transmission.
3. When the wired peripheral interface establishes the data connection, it should give the user the corresponding state change prompt, such as the indicator light change, when the conditions permit.
4. For the interface with debugging function, epoxy resin coating shall be added at the interface to prevent reverse engineering (optional).

5.1.2. Chip and module

1. Have function of physical write protection to prevent the firmware from being tampered.
2. Support the trusted execution environment, provide the isolation of security domian and non-security domian (optional).
3. The security module of device hardware has environmental failure protection (RFP) or environmental failure test (EFT).
4. The device hardware can effectively preventthe the failure attacks, for instance damage of voltage, temperature and other environmental anomalies to the module security.

5.2. Firmware/Operating System security advices

5.2.1. System upgrade

1. At least have the ability to update automatically or manually.
2. For the device that updates the system through OTA, when the download source is configurable, the system can validate the legitimacy of the download source.
3. The firmware source provides firmware verification data to ensure that the system can confirm the integrity of the firmware before upgrading.
4. When the system automatically updates failed, system can roll back to the previous version and remind the user.
5. The system has the ability to eliminate serious security vulnerabilities through patches or software upgrades, to ensure that the system vulnerabilities can be repaired in time.

5.2.2. System Permission Restrictions

1. For the system that supports multiple user accounts, the user authority assignment follows the principle of minimum authority.User can access the system only after authentication and only authorized accesses are allowed.
2. The remote-control request of the system has the ability of identity authentication and access

authentication, to avoid illegal users or application control system, resulting in the system being illegally controlled.

3. The system needs to obtain the user's authorization when installing the applications.The system shall not install applications not authorized by the user. When the application is installed, the minimum authorization principle is adopted in the permission allocation, and the system can prohibit the use of all unauthorized permissions.

4. The system implements appropriate access control management measures for different application processes and data, and the processes and data of different applications cannot be freely accessed. (optional)

5.2.3. Bootup authentication

1. The secure boot mechanism should be provided so that the system cannot start up unless the firmware passed Integrity and authenticity verification.

5.2.4. Service configuration

1. The system service authorization follows the principle of minimization. Besides the necessary service ports, the number of open ports should be reduced as far as possible. The telnet port is closed by default, and the SSH Remote Login port is closed by default.

2. For the system that can install external applications, the access control mechanism of system API such as location and network access is provided to prevent the application from unauthorized calling the system interface.

3. For the system with configurable services, it has the function of modifying the default configuration. The specific functional requirements include but are not limited to modifying the default identity and authentication information, enabling and disabling services, application access restrictions and application background refresh, data upload, data download restrictions and monitoring.

4. The system shall provide the Indicator of data communication connection status.

5. For the equipment with remote connection, the system uses secure communication protocol to protect the security of management channel.

5.2.5. System configuration

1. Except updating, diagnostic, or maintenance, the key partition (boot partition, system partition)shall be set to read-only mode.

2. For the device with debugging function, strictly limit the permission of debugging process in the operating system to prevent the abuse of permission caused by high permission setting.

3. For the equipment with debugging-mode, the debug ports such as ADB are closed by default, and the ability to configure the debugging interface switch state through local or remote mode is provided to improve the controllability of debugging function.

4. For devices with USB interface, the function of USB debugging interface is turned off or hidden by default, or debugging interface verification is added.

5. Secure GUI is recommended.

5.2.6. Partition and debug configuration

1. For devices with debug function, debug ports such as ADBD port should be turned off by default.

2. For devices with USB ports, the USB debug interface should be turned off or hidden by default, verification is needed when turned on.

5.2.7. Encryption and Authentication

1. The system shall have fast encryption capability matching 5G network speed.
2. The system has high-level authentication capability.
3. The system has high-level end-to-end encryption capability.
4. The system has high-level information integrity protection capability.

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

5.3. Application security advices

5.3.1. Built-in application

1. For the built-in application with remote connection function, it has the ability to authenticate the application requesting remote connection, so as to avoid the application being illegally connected and controlled.
2. The user password and user authentication information are encrypted, and it is forbidden to record sensitive information in the log and configuration file.
3. For the same device with multiple user accounts, it has access control function to prevent unauthorized operation of other user data.
4. It has the mechanism to modify the default password.
5. Avoid hard coded cryptography keys in code.
6. When the built-in application is updated, the ability to upgrade from the official channel is provided by default, and the integrity and source legitimacy of the installation package can be verified.

5.3.2. Client application

1. The user password and user authentication information are encrypted, and it is forbidden to record sensitive information in the log and configuration file.
2. If the application interacts with the cloud, the two-way authentication should be carried out before transmission, and the communication data should also be encrypted.
3. The application encrypts and stores the user's sensitive information uploaded by the device.
4. The user login verification module has the ability to prevent violent attacks of authentication.
5. In the case of authentication failure, the system can provide users with general error information to avoid this error information being exploited by attackers.
6. In any case, it is not allowed to maliciously control the device or read the device data without explicitly prompting the user or without the permission of the user.
7. It is not allowed to update the program forcibly. There is a prompt before updating, and the foreground will display when updating, except that the user sets "automatic update without prompt".

5.3.3. Client application security requirements under eMBB

1. The user password and user authentication information are encrypted, and it is forbidden to record sensitive information in the log and configuration file.

5.4. Data security advices

5.4.1. Data Transmission

1. The ability to protect sensitive data is needed when transmitting data. By means of encryption, the confidentiality, integrity and validity of data will be ensured.

5.4.2. Data Storage

1. The ability to protect sensitive data in the process of generating, storing, transmitting, destroying, backing up, and recovering is needed.
2. The application context file (including configuration files, databases, cookies, etc.), should not store the DB password, FTP service password, login password, external system interface authentication password and other sensitive data.
3. The user password and user authentication information shall be securely stored to protect confidentiality and integrity.It is forbidden to record sensitive information in the log and configuration file, and it is forbidden to record sensitive information in the log and configuration file.

5.4.3. Access Control

1. For systems that support multiple-account, the ability to isolate sensitive information fromdifferent users is needed.
2. For systems that support third-party applications installation, the ability to detect or record unauthorized data access is needed.

5.4.4. Log

1. 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.
2. Secure login information needs to be encrypted.
3. 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.
4. Unexpected shut down, restart, file system collapse of device should be logged automatically.
5. The privilege of reading, modifying, and deleting logs should be only assigned to the administrators.