GTI Security Test Guide for IoT Device

GTI Security Test Guide for IoT Device

Version:	V1.0.0
Deliverable Type	□ **Procedural Document** ☑**Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** ☑ **Open to Public**
Working Group	Terminal WG
Task	PM3-PJ9-task5: Security test Guide for IoT device
Source members	CMCC
Support members	
Editor	CMCC
Last Edit Date	2018-12-18
Approval Date	25-01-2019

Document History

Date	Meeting #	Version #	Revision Contents
DD-MM-YYYY		NA	
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			

Table of Contents

1 Executive Summary 5
2 Abbreviations 6
3 References 7
4 Test Environment 8
5 Hardware Security Test 8
6 System Security Test 8
7 Application Security Test 10
8 Data Security Test 11

1 Executive Summary

The IoT devices provide the access to the data of the whole IoT system , the IoT devices security is one of the most important parts of IoT security . This white paper focuses on the major security of IoT devices.

The purpose of this document is to enable the suppliers of IoT products , services and components to assess the conformance of their products, services and components to the GTI Security test Guide for IoT device . Completing a GTI Security Assessment will allow an entity to demonstrate the security measures they have taken to protect their products .

2 Abbreviations

Abbreviation	Explanation
IoT	Internet of Things
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 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 IoT devices

4 Test Environment

Test Environment is shown in the Figure1, including IoT device , smart phone , service platform , computer and other auxiliary tools (such as UART tool etc.). smart phone , IoT 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.

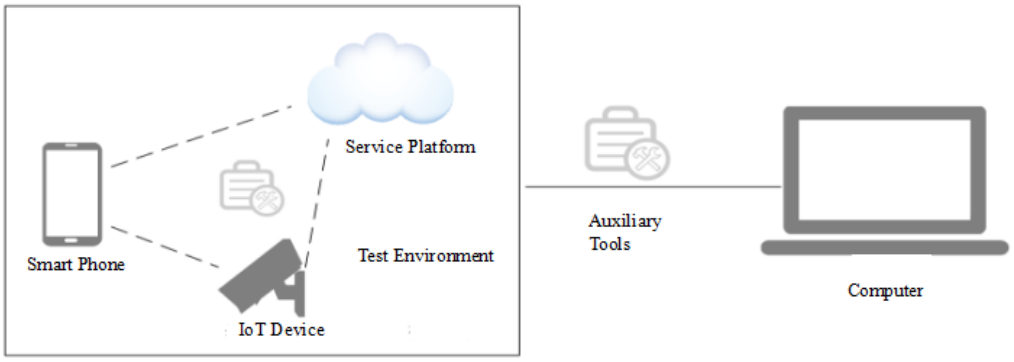

Figure 1 A simple Diagram of Test Environment

5 Hardware Security Test

Task code	Description	Test procedure
Hardware security Debug port-01	The identity Authentication is needed for devices with debug port to prevent direct login.	• Restore device to factory settings; • If debug port is available,try to login through the debug port 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☐	

6 System Security Test

Task code	Description	Test procedure
System security	The multi-user system design	Prerequisite:The system design

System Privilege Restrictions-01	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 .	documentation is needed. • Check the system design documentation to determine whether multi-user is available . • 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. • Check the system design documentation to determine the path of important partition . •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. • Check the system design documentation to determine the privilege of debug port . • 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	Prerequisite:The system design documentation is needed. • Check the system design documentation to determine the

	should be minimized	necessary service port . • 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. 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.	• Restore device to factory settings; • Try to modify the default system configuration .
Task result	The default system configuration can be modified . Yes☐ Part☐ No ☐ N/A☐	

7 Application Security Test

Task code	Description	Test procedure
Application Security Pre-installed application-02	The use of hard-coded password should be avoided.	• Extracting file system from the firmware . • 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. • Use the device for a period of time normally . • Check the important files to determine whether unencrypted sensitive information exist .
Task result	Unencrypted sensitive information is 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. • Use the device for a period of time normally . •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,	Prerequisite:The path of system log is needed. • Use the device for a period of

	operating content and operating results.	time normally . •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. • Use the device for a period of time normally , and cut the power . •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☐	