GTI Security Technical Implementation Guide for IoT devices

http://www.gtigroup.org

Security Technical Implementation Guide for IoT 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	IoT
Project Name	Security
Source members	CMCC
Support members	Huawei
Editor	QIguang Fan , Wenjie QI ,
Last Edit Date	10-06-2018
Approval Date	10-06-2018

Document History

Date	Meeting #	Revision Contents	Old	New

Table of Contents

1. Introduction

The Internet of Things(IoT) is changing how people live in ways never seen before,from fitness tracker and VR glasses to smart thermostats,intelligent streetlight,water monitors,and more,the IoT is in more place than ever.

With the rise of Smart devices technology, the IoT market has been presenting an exponential growth trend, the interconnection of all things has become an inevitable trend of technology development and industrial application.In 2020, according to Gartner's prediction , the number of devices in the Internet of things worldwide will reach to 26 billion.At the same time, the Internet of things security incidents are showing an explosive growth trend, security threats continue to deteriorate.Many countries hve been starting to enhance the security of the Internet of things from the strategic, standards, regulatory and other levels of attention.At the end of 2016, the US Department of Homeland Security issued the "Strategic principles for securing the Internet of things," and a senior Homeland Security official said publicly that "Internet of things security has evolved into a homeland security issue.".At the same time, the European Union also have announced to speed up the pace of development of Internet of things security regulations.

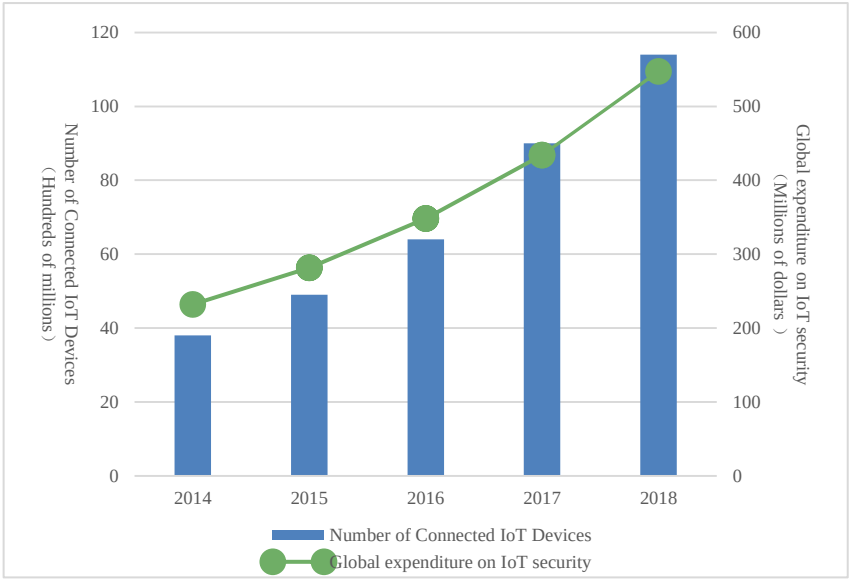

Fig. 1 Gartner's prediction on IoT security

The IoT brings a new set of issues, such as the security, safety of cyber-physical systems. Novel types of attack may take many industries by surprise.To succeed with the transformation that the IoT brings about, industries need to gather competence and understand new threats and how to mitigate them.

The security ability is not evenly distributed in IoT industry , showing a phenomenon of ‘top heavy’，manufacturers pay more attention on service platform,because the IoT service platform is not very different from traditional service platform,which generally have considered the information security at the beginning of design and the protective measures also have the corresponding standard. All kinds of terminals in the perceptual layer are generally weak because of the large number of terminals or the limitation of resource and technical ability, which have become the weak link of the information security of the Internet of things system.

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 requirements set forth below are designed to improve security of IoT devices,Widespread adoption of these strategic principles and the associated suggested practices would dramatically improve the security of IoT devices.

2. IoT devices Security Model

The Security Technical Implementation Guide for IoT devices defines the standard IoT devices model shown in the diagram below. This model comprises four principle components – the IoT devices hardware security,the IoT devices firmware/operating system security,the IoT devices application security and the IoT devices data security.

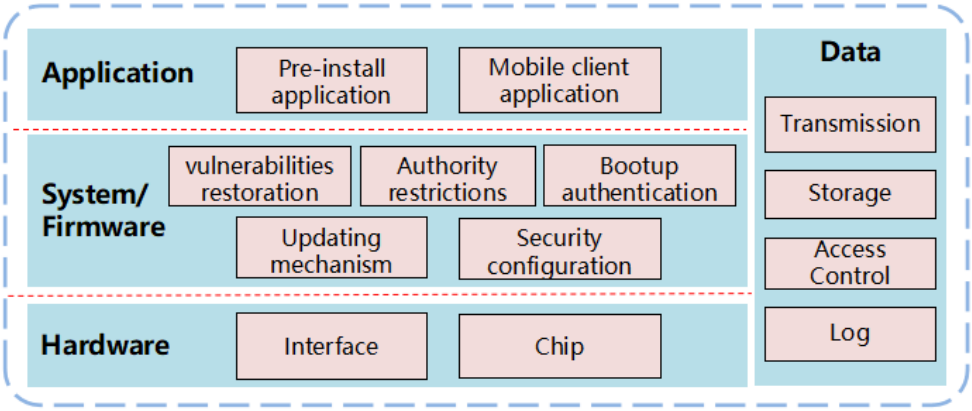

Fig. 2 The standard IoT device mode

3. Risks analysis

3.1 Types of Risks to hardware of IoT devices

Threat 1： 80% Of the IoT devices exposes the debug interface, which can be used by hackers to break the device's running mechanism and update the firmware.

Threat 2： A critical chip may cause the chip to enter an abnormal working state due to an attacker's input of a specific voltage.

3.2 Types of Risks to firmware/operating system of IoT devices

Threat 3: The system is not updated in a timely manner or the update system is imperfect.As the low terminal system version equipped in the Internet of things, the possible and known system vulnerabilities or the imperfect security mechanisms in the process of system upgrade s will lead to the result that the upgrade process may be used or attacked by hackers.

Threat 4: Privilege abuse.System permissions open too much or the restriction on the authority is not strict, resulting in an attacker can directly or indirectly call the way to achieve the attack effect.

Threat 5: No certification on system security's booting.IoT terminal start-up code is not verified for integrity and there is a bug in the boot process, which will be used by hackers to write firmware.

Threat 6: Imperfection of the system configuration security

The imperfection of system partition configuration and allocation of authority, resulting in the possibility of system intrusion, remote control or used by hacker for firmware refresh.

3.3 Types of Risks to application of IoT devices

Threat 7: Because the protective measures applied on IOT equipment are not enough and the operating environment is complex, there may be risks such as authentication being bypassed, data leaking, injected and controlled, etc.

3.4 Types of Risks to data of IoT devices

Threat 8: The firmware stores sensitive information such as passwords and secret keys, which may lead to remote control of the devices.

Threat 9: Improper setting of data access authorities may cause unnecessary data leak.

Threat 10: For the IoT terminal which supports the external storage devices, the risk of data leakage may be caused when the application software is authorized to store, move, copy and transfer the important data to the external storage devices.

Threat 11: For IoT terminals that support peripheral interfaces, the abuse of input and output functions and authorities may result in the risk of devices data leakage and illegal intrusion.

4. Definitions and abbreviations

Definitions

IoT device: An IoT device is any nonstandard computing devices that connects wirelessly to a network and has the ability to transmit data; these are the things in the Internet of Things.

Abbreviations

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

5. General security advices for IoT devices

5.1.Hardware security advices

5.1.1.Interface

1. The identity Authentication is needed for devices with console interface to prevent direct login.
2. When the wireless data interface establishes a data connection,The ability to display data transfer status such as indicator light and display is needed to prevent illegal access,illegal data transmission,etc.
3. When the wired data interface establishes a data connection,The ability to display data transfer status is needed for devices with display function to prevent illegal access,illegal data transmission,etc.
4. The hardware debug interface should be covered by epoxy resin coating to prevent from firmware reverse engineering.(optional)

5.1.2.Chip

1. The write-protected function of the chips that stores firmware is necessary to prevent the firmware from being tempered with.
2. The Trust Execution Environment should be supported to provides security features such as isolated execution,integrity of applications etc..

5.2.Firmware/Operating System advices

5.2.1.System upgrade

1. The ability of automatically or manually upgrade is necessary.
2. The ability to verify the authenticity of firmware upgrades is needed.
3. When the system upgrade process is interrupted, the ability to revert to the pre-upgrade version is necessary.
4. The operating system should have the ability to eliminate serious security vulnerabilities by means of patches or software updates. Once, the system vulnerabilities are founded, they should be fixed in time.

5.2.2. Privilege Restrictions

1. 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.
2. The ability to verify the request of remote control is needed to prevent unauthorized login.
3. Application can only be installed with users' permission.Application installation should follow the Principle Of Least Privilege and the default application should be prohibited from getting root permissions.
4. Appropriate access control mechanisms is needed for processes and data of different applications,so that they can not be accessed at will.

5.2.3. Bootup authentication

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

5.2.4.Service configuration

1. System services should follow the principle of least privilege.In addition to the necessary service port, the number of open ports should be minimized.
2. For systems that can install third-party applications, access control mechanisms for system APIs such as location and network access should be provided to prevent unauthorized system calls.
3. 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.
4. The ability to provide signal for data transmission status is necessary.
5. To ensure the security of system with remote management function, a secure communication protocol should be applied to channel management .

5.2.5. Partition and debug configuration

1. The important partition（boot、system）should be configured as read-only mode.
2. 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.
3. For devices with debug function,debug ports such as ADBD port should be turned off by default.
4. For devices with USB ports, the USB debug interface should be turned off or hidden by default, verification is needed when turned on.

5.3.Application advices

5.3.1.Pre-installed application

1. For applications that support remote connection,the ability to authenticate the application request is needed to prevent unauthorized connections.
2. The function of securely encrypt sensitive information is needed, explicitly record sensitive information in logs and configuration files should be forbidden.
3. Access control functions based on the role is necessary to prevent unauthorized operations on other user’s private data.
4. The function of modifying the default password is necessary.
5. The use of hard-coded password should be avoided.
6. The ability to upgrade the pre-installed application from official site by default is necessary,the data integrity and source installation package should be verified.

5.3.2.Mobile Apps

1. The function of securely encrypt sensitive information is needed, explicitly record sensitive information in logs and configuration files should be forbidden.
2. The data transmission between apps and devices should be encrypted.
3. The mutual authentication between Apps and cloud is needed before data transmission,and the data transmission between Apps and cloud should be encrypted.
4. The ability to prevent Brute Force is needed for the login module.
5. The authentication error message should not disclose too many information to prevent abusing.
6. Notice or user's confirmation before update is needed,otherwise the update will not be applied,except the user chose 'automatic update without notice'.

5.4.Data 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.

5.4.3.Access Control

1. For systems that support multiple-account,the ability to isolate sensitive information from other data 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. 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.
3. Unexpected shut down, restart,file system collapse of device should be logged automatically.
4. The privilege of reading, modifying, and deleting logs should be assigned by accounts.